

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor : Shinya YAMAMURA,et al.
Filed : Concurrently herewith
For : PROXY NETWORK CONTROL
Serial No. : Concurrently herewith

November 25, 2003

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRIORITY CLAIM AND
SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-346949** filed **November 29, 2002**, a certified copy of which is enclosed.

Respectfully submitted,



Thomas J. Bean
Reg. No. 44,528

Katten Muchin Zavis Rosenman
575 Madison Avenue
New York, NY 10022-2585
(212) 940-8800
Docket No.: FUJH 20.761



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 2 9 日
Date of Application:

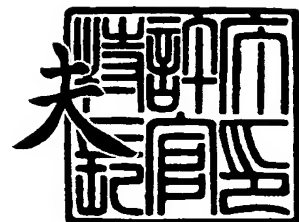
出 願 番 号 特 願 2 0 0 2 - 3 4 6 9 4 9
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 4 6 9 4 9]

出 願 人 富 士 通 株 式 会 社
Applicant(s):

2 0 0 3 年 8 月 1 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

今 井 康



出 証 番 号 出 証 特 2 0 0 3 - 3 0 6 1 9 1 3

【書類名】 特許願

【整理番号】 0253396

【提出日】 平成14年11月29日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/24
H04L 12/66
G06F 13/00

【発明の名称】 代理ネットワーク制御装置

【請求項の数】 10

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

【氏名】 山村 新也

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

【氏名】 佐藤 義治

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

【氏名】 中村 勝一

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

【氏名】 堀口 辰雄

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100094514

【弁理士】

【氏名又は名称】 林 恒徳

【選任した代理人】

【識別番号】 100094525

【弁理士】

【氏名又は名称】 土井 健二

【手数料の表示】

【予納台帳番号】 030708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 代理ネットワーク制御装置

【特許請求の範囲】

【請求項 1】 ユーザ端末に所定のサービスを提供するサービス装置に代行して、該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置であって、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と、

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定して実行する実行部と、

を備えている代理ネットワーク制御装置。

【請求項 2】 ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行する代理ネットワーク制御装置であって、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と、

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定するサービス制御部と、

前記サービス制御部により決定された機能に基づいて前記ネットワーク装置を制御する外部機器制御部と、

を備えている代理ネットワーク制御装置。

【請求項 3】 請求項 2 において、

前記サービス装置は D H C P サーバであり、

前記パケット監視部は、前記サービス装置から前記ユーザ端末に発行されるアドレスを含んだパケットを監視し、

前記サービス制御部は、前記パケット監視部により監視されたパケットに基づいて、前記サービス装置により発行されたアドレスを送信元アドレスとして有す

るパケットを通過させ、それ以外のアドレスを送信元アドレスとして有するパケットを通過させないアクセス規制機能を決定し、

前記外部機器制御部は、前記アクセス規制機能を実行するように前記ネットワーク装置を制御する、

代理ネットワーク制御装置。

【請求項 4】 請求項 2 において、

前記ユーザ端末がホームネットワークのホームアドレスを有する移動通信端末であり、前記ネットワーク装置が前記ホームネットワークの外部ネットワークから外部に送信されるパケットのうち、所定の送信元アドレスを有するパケットを通過させ、それ以外のパケットを通過させないファイアウォールであり、

前記パケット監視部は、前記外部ネットワークに移動した前記ユーザ端末と前記ホームネットワークのホームエージェントとの間で通信される、前記ユーザ端末のホームアドレスを含んだパケットを監視し、

前記サービス制御部は、前記パケット監視部により監視されたパケットに基づいて、前記ホームアドレスを有するパケットを通過させるようにアクセス規制を解除する機能を決定し、

前記外部機器制御部は、前記アクセス規制を解除する機能を実行するように、前記ネットワーク装置を制御する、

代理ネットワーク制御装置。

【請求項 5】 請求項 2 において、

前記ユーザ端末が I P v 6 端末であり、前記サービス装置が生成された前記ユーザ端末の I P アドレスの認証を行う認証サーバであり、

前記パケット監視部は、前記サービス装置により認証された I P アドレスを含むパケットを監視し、

前記サービス制御部は、前記パケット監視部により監視されたパケットに基づいて、前記 I P アドレスを送信元アドレスとして有するパケットを通過させるようにアクセス規制を解除する機能を決定し、

前記外部機器制御部は、前記アクセス規制を解除する機能を実行するように、前記ネットワーク装置を制御する、

代理ネットワーク制御装置。

【請求項 6】 コンピュータに、

ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間で通信されるパケットを監視する手順と、

前記監視したパケットに基づいて、前記サービス装置に代行して、該サービス装置の機能を補完または拡張する機能を決定して実行する手順と、

を実行させるためのプログラム。

【請求項 7】 ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行するコンピュータに、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視する手順と、

前記監視したパケットに基づいて前記補完または拡張する機能を決定する手順と、

前記決定した機能に基づいて前記ネットワーク装置を制御する手順と、

を実行させるためのプログラム。

【請求項 8】 ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し、所定の条件を満たすパケットに基づいて、前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と、

を備えているネットワークシステム。

【請求項 9】 ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と、

前記ユーザ端末と前記サービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置と、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し、所

定の条件を満たすパケットに基づいて前記ネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と、

を備えているネットワークシステム。

【請求項 1 0】 請求項 9 において、

前記サービス装置は D H C P サーバであり、

前記代理ネットワーク制御装置は、前記サービス装置から前記ユーザ端末に配布されるアドレスを含んだパケットを監視し、前記ユーザ端末から送信される、前記アドレスを送信元アドレスとして有するパケットを通過させ、それ以外のパケットを通過させないように前記ネットワーク装置を制御する、

ネットワークシステム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ネットワークの機能を代理実行する代理ネットワーク制御装置に関し、特に、ユーザ端末に所定のサービスを提供するサービス装置に代行して、該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置に関する。

【 0 0 0 2 】

また、本発明は、ネットワークの機能を代理実行するコンピュータに実行させるためのプログラムに関し、特に、ユーザ端末に所定のサービスを提供するサービス装置に代行して、該サービス装置の機能を補完または拡張する機能をコンピュータに実行させるためのプログラムに関する。

【 0 0 0 3 】

さらに、本発明は、このような代理ネットワーク制御装置を有するネットワークシステムに関する。

【 0 0 0 4 】

【従来の技術】

インターネット（I P ネットワーク）の普及に伴い、どこからでも自由に I P

ネットワークに接続できるような環境が整いつつある。このような環境は、ネットワークを利用するユーザにとって利便性が向上する一方で、ネットワークを管理する側にとって誰でもネットワークに接続できるので、セキュリティの観点から問題がある。

【 0 0 0 5 】

特に、D H C P (Dynamic Host Configuration Protocol) や I P v 6 等のプロトコルによると、アドレスが自動的に作成されユーザに発行されるので、ユーザはアクセスする場所のアドレス情報を知らなくても、ネットワークにアクセスできる。

【 0 0 0 6 】

したがって、今後、セキュリティの観点から、アクセス権限を有しないユーザのアクセスを制限するアクセス規制が重要となってくる。

【 0 0 0 7 】

アクセス規制を行うため、アクセス規制機能を有するネットワーク装置とユーザの認証を行う認証装置とを組み合わせたり、D H C P を実行する D H C P サーバにネットワーク装置の制御機能を付加することによりアクセス規制を行う提案が行われ、製品も登場しつつある（例えば特許文献 1 ～ 4 参照）。

【 0 0 0 8 】

また、端末のネットワークへの接続を制御する方式としては、制御サーバ（認証サーバ、D H C P サーバ等）と制御装置（ファイアウォール、パケットシェーピング装置等）とを組み合わせ、ユーザを認証後、ユーザ端末からネットワークへの接続を許容することが従来の技術で行われている。

【 0 0 0 9 】

ネットワークの機能を代理実行するものとしては、W E B コンテンツをキャッシュし、コンテンツのオリジナルを提供しているサーバとは別のサーバが代理で W E B コンテンツをユーザに提供するプロキシサーバがある。プロキシサーバは、利用ユーザが明示的にサーバのアドレスを指定するものと、ネットワーク側で強制的にパケットを捕捉し、プロキシサーバの機能を実行する透過型プロキシとがある。

【 0 0 1 0 】

ネットワークの制御を，所定の指針で行う仕組みとしてはポリシーベースネットワーク（P B N : Policy Based Network）がある。P B N は，指定されたパケットを捕捉するポリシーデテクションポイントと，捕捉したパケットに対するポリシー（動作）を決定するポリシーサーバと，決定されたポリシーに基づき該当するトラフィックの制御を行うポリシー実施ポイントとで構成される。

【 0 0 1 1 】

トラフィックを監視するものとしては，sniffer, etherealといったプロトコルモニタが存在する。

【 0 0 1 2 】

【特許文献 1】

特開 2 0 0 1 - 3 2 6 6 9 6 号公報

【 0 0 1 3 】

【特許文献 2】

特開 2 0 0 1 - 3 6 5 6 1 号公報

【 0 0 1 4 】

【特許文献 3】

特開 2 0 0 1 - 2 7 4 8 0 6 号公報

【 0 0 1 5 】

【特許文献 4】

特開平 1 1 - 2 4 3 3 8 9 号公報

【 0 0 1 6 】

【発明が解決しようとする課題】

しかし，D H C P サーバに新たな機能を追加する場合には，これまで使用していた D H C P サーバを新たなものに変更したり，既存の D H C P サーバのプログラムやハードウェアを変更したりする必要がある，また，既存のネットワーク構成そのものを変更しなければならない場合もある。さらに，I P v 6 については，提案のみがなされており，装置は存在しないのが実情である。

【 0 0 1 7 】

また、認証サーバと制御装置を組み合わせる方式は、認証サーバが制御装置に対して、アクセス規制を行うため、認証サーバと制御装置の組み合わせは、認証サーバの制御ソフトによって決定されてしまう。そのためアクセス規制サービスを導入しようとするネットワーク運営者は、新たな認証サーバと制御装置とをセットで購入しネットワークに組み込む必要があり、コストが高くなる。

【 0 0 1 8 】

プロキシサーバは、主に H T T P プロトコル専用で作られており、H T T P 以外には、R T P 等、限られたプロトコルしかサポートしていない。また、プロキシサーバは、キャッシュされている情報をユーザからの H T T P リクエストへの応答として答えるか、コンテンツのオリジナルを格納しているサーバへ、ユーザ端末の代理として通信を行うかのいずれかの機能しか有しておらず、特定のサービスを補完するような機能を有しない。

【 0 0 1 9 】

また、透過型プロキシは H T T P プロトコルを強制的に横取りしているが、あくまでもプロキシサーバ内部で処理を終端しており、通常のプロキシと動作は変わらない。さらに、プロキシサーバは、アクセス規制に使用する情報が U R L であり、ネットワークへのアクセス規制とは異なる機能しか実行できない。

【 0 0 2 0 】

P B N は、パケットを監視し、所定の指針に基づき、パケットを制御するが、パケット監視装置とポリシーサーバとをネットワークに導入しなければならない。したがって、P B N によると、ネットワークに新たな装置を導入し、またネットワークの構成の変更を伴う。

【 0 0 2 1 】

また、P B N では、ポリシーを決定するための条件は、I P アドレスやポート番号等の I P ヘッダの情報に依存しており、一般にプロトコルの詳細までを解析して動作するようにはなっていない。

【 0 0 2 2 】

プロトコルモニタは、プロトコルを表示用に解析する機能は持っているが、解析したプロトコルを基に、何らかの動作を行う機能や、ネットワーク機器との連

携機能を具備しない。

【0023】

本発明は、このような背景に鑑みなされたものであり、その目的は、ネットワークの既存の装置やネットワークの構成に変更を加えることなく、ネットワークの機能、特にユーザ端末にサービスを提供するサービス装置の機能を補完または拡張することができる代理ネットワーク制御装置および該代理ネットワーク制御装置を有するネットワークシステムを提供することにある。

【0024】

【課題を解決するための手段】

前記目的を達成するために、本発明による代理ネットワーク制御装置は、ユーザ端末に所定のサービスを提供するサービス装置に代行して、該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置であって、前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と、前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定して実行する実行部と、を備えている。

【0025】

また、本発明による代理ネットワーク制御装置は、ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行する代理ネットワーク制御装置であって、前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と、前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定するサービス制御部と、前記サービス制御部により決定された機能に基づいて前記ネットワーク装置を制御する外部機器制御部と、を備えている。

【0026】

本発明によると、代理ネットワーク制御装置が、サービス装置に代わって、サービス装置の機能を補完または拡張する機能を代理実行するので、サービス装置

に機能を追加したり、サービス装置を新たなものに交換したりする必要がない。これにより、既存のネットワーク資源をそのまま使用することができ、コストを削減することができる。また、代理ネットワーク制御装置は、サービス装置とユーザ端末との間で通信されるパケットを監視できる場所であれば、どこでも設置することができる。例えばネットワーク装置が有する監視インタフェース等に代理ネットワーク制御装置を接続することができる。これにより、ネットワークの構成を変更することなく、代理ネットワーク制御装置を既存のネットワークに組み込むことができる。

【0027】

本発明によるネットワークシステムは、ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と、前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し、所定の条件を満たすパケットに基づいて、前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と、を備えている。

【0028】

本発明によるプログラムは、コンピュータに、ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間で通信されるパケットを監視する手順と、前記監視したパケットに基づいて、前記サービス装置に代行して、該サービス装置の機能を補完または拡張する機能を決定して実行する手順と、を実行させるためのものである。

【0029】

また、本発明によるプログラムは、ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行するコンピュータに、前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視する手順と、前記監視したパケットに基づいて前記補完または拡張する機能を決定する手順と、前記決定した機能に基づいて前記ネットワーク装置を制御する手順と、を実行させるためのものである。

【0030】

本発明によるプログラムによっても、上記本発明による代理ネットワーク制御装置と同様の作用効果を得ることができる。

【0031】

本発明によるネットワークシステムは、ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と、前記ユーザ端末と前記サービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置と、前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し、所定の条件を満たすパケットに基づいて前記ネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と、を備えている。

【0032】

本発明によるネットワークシステムによっても、前記同様に、既存のネットワーク資源を変更することなく使用でき、また、ネットワークの構成を変更することなく、代理ネットワーク制御装置をネットワークに組み込むことができる。

【0033】**【発明の実施の形態】****<ネットワークシステムの構成>**

図1 (A) ～ (D) は、本発明の実施の形態による代理ネットワーク制御装置 (PNCU: Proxy Network Control Unit) を有するネットワークシステムの構成例を示すブロック図である。

【0034】

図1 (A) , (C) , および (D) に示すネットワークシステムは、PNCU 1, サービスサーバ2, ユーザ端末3, およびネットワーク4 に設けられた1または2以上 (図1 (A) ～ (D) ではn個: nは正の整数) のネットワーク機器41～4nを有する。また、図1 (B) に示すネットワークシステムは、これらの構成要素に加えてハブ5をさらに有する。

【0035】

ネットワーク4は、例えばIPネットワークであり、IPパケットを転送する

ためのネットワーク機器 4 1 ～ 4 n により構成される。ネットワーク機器 4 1 ～ 4 n は、パケットを転送する装置であり、例えばルータ、ハブ、L 3 スイッチ（レイヤ 3 スイッチ）、ファイアウォール、ゲートウェイサーバ、N A T（Network Address Translation）サーバ、N A P T（Network Address Port Translation）サーバ、プロキシサーバ等を含む。

【 0 0 3 6 】

ユーザ端末 3 は、ネットワーク 4 を介してサービスサーバ 2 と通信を行い、サービスサーバ 2 からサービスの提供を受ける端末である。ユーザ端末 3 として、例えばデスクトップ P C、ノート P C、P D A（Personal Digital Assistant）等がある。

【 0 0 3 7 】

サービスサーバ 2 は、ユーザ端末 3 からの要求に応じて、様々なサービスをユーザ端末 3 に提供するサーバである。サービスサーバ 2 として、例えば情報を提供する W E Bサーバに加えて、ネットワークアクセスやネットワーク制御等を行う D H C Pサーバ、認証サーバ、ポリシーサーバ等がある。

【 0 0 3 8 】

ユーザ端末 3 とサービスサーバ 2 との間では、サービス用プロトコルにより通信が行われ、ユーザ端末 3 はサービスサーバ 2 よりサービスを受けることができる。サービス用プログラムとして、例えば自動 I P アドレス割付けサービスのための D H C P（Dynamic Host Configuration Protocol）や、認証サービスのための認証プロトコル等がある。

【 0 0 3 9 】

P N C U 1 は、ネットワーク機器 4 1 ～ 4 n の一部または全てを制御して、既存のネットワークにある装置（例えばサービスサーバ 2、ネットワーク機器 4 1 ～ 4 n、ハブ 5、ユーザ端末 3 等）や構成を変更することなく、既存のネットワークにない機能を補うための装置（またはプログラム）である。既存のネットワークに補う機能としては、ネットワークセキュリティの確保（例えばネットワークに登録されていない者のネットワークへのアクセスの排除等）、モバイル I P におけるファイアウォールのパケットの通信確保（ファイアウォールの穴あけ）

等がある。

【0040】

PNCU1は、既存のネットワークにある装置や構成を変更することなく、既存のネットワークにない機能を補完するので、ネットワークの構成要素の変更や構成の変更に伴うコストを削減することができる。PNCU1の詳細な構成については後に詳述する。

【0041】

ネットワーク機器41～4nを制御するために、PNCU1とネットワーク機器41～4nとの間では、機器制御用プロトコルによる通信が行われる。この機器制御用プロトコルとして、例えば、Telnetによるコマンドラインインタフェース、SNMP (Simple Network Management Protocol) 等がある。

【0042】

PNCU1は、機能補完を行うためには、ユーザ端末3とサービスサーバ2との間で通信されるパケットを監視する。このようなPNCU1による全パケットの監視は、図1 (A) ～ (D) のいずれの構成によっても行うことができる。

【0043】

すなわち、図1 (A) に示す構成例1では、PNCU1がユーザ端末3とサービスサーバ2との間の通信経路上に挿入され、ユーザ端末3とサービスサーバ1との間のすべてのトラフィック (メッセージ、パケット) がPNCU1を経由して通信される。したがって、PNCU1は、ユーザ端末3とサービスサーバ2との間で通信される全てのパケットを監視することができる。

【0044】

図1 (B) に示す構成例2では、ネットワーク機器4nとサービスサーバ2との間に、複数のユーザ端末またはサーバを集線するネットワーク装置であるハブ5が設けられ、PNCU1はサービスサーバ2が接続されたハブ5に接続される。この構成では、ハブ5からサービスサーバ2又はユーザ端末3に送信されるパケットが、ハブ5に接続された全ての装置に伝送レイヤ (OSI階層モデルのレイヤ2) でブロードキャストされる。したがって、PNCU1は、ユーザ端末3とサービスサーバ2との間で通信されるパケットを受信し、監視することができ

る。なお、ハブ5は、ユーザ端末3とネットワーク機器41との間に設けられてもよい。

【0045】

図1(C)に示す構成例3では、PNCU1がユーザ端末3とサービスサーバ2との間の通信経路に存在するいずれかのネットワーク機器(図1(C)ではネットワーク機器4n)の監視インタフェースに接続される。ネットワーク機器の監視インタフェースは、パケットを監視するためのインタフェースであり、ネットワーク機器を経由する全てのパケットが監視インタフェースから出力される。したがって、この構成でも、PNCU1はユーザ端末3とサービスサーバ2との間で通信されるパケットを監視することができる。

【0046】

図1(D)に示す構成例4では、PNCU1がサービスサーバ2に組み込まれる。例えばPNCU1はプログラムにより実現され、サービスサーバ2上で起動される。この構成によっても、PNCU1は、サービスサーバ2とユーザ端末3との間で通信されるパケットを監視することができる。

【0047】

<PNCUの構成>

図2は、PNCU1の機能ブロック図である。PNCU1は、アドレスリスト11、サービス管理テーブル14、アクセスリスト111、初期設定処理部12、パケット監視部13、サービス制御部16、ロギング機能部17、通知メッセージ制御部18、周期処理部19、外部機器制御部110、プロトコルライブラリ15、およびコマンドラインインタフェース(CLI: Command Line Interface)ライブラリ112を有する。

【0048】

各機能ブロックはプログラムにより構成することもできるし、ハードウェア回路により構成することもできる。各機能ブロックがプログラムにより構成された場合には、このプログラムは、PNCU1の起動時にPNCU1の不揮発性メモリ(ハードディスク等)から半導体メモリ(RAM等)に呼び込まれ、PNCU1のCPUにより実行される。

【0049】

アドレスリスト11は、PNCU1の起動時に、初期設定動作の対象を決定するために参照されるデータであり、例えば不揮発性メモリ（ハードディスク等）に記憶される。

【0050】

図3は、アドレスリスト11の構成例を示している。アドレスリスト11は複数のエントリを有する。各エントリは、PNCU1が提供するサービス（ネットワークに補完する機能）の種別を示すサービスタイプと、複数のサービス固有情報とを有する。各サービス固有情報は、例えばアクセス規制を行う対象となるユーザ端末のIPアドレスである。

【0051】

サービス管理テーブル14は、サービスタイプ毎の処理決定テーブルへのポインタをエントリとして持つトランザクションであり、例えば揮発性メモリ（RAM等）に記憶され、その内容はPNCU1の動作によって動的に変更される。

【0052】

図4は、サービス管理テーブル14の構成例を示している。サービス管理テーブル14は、サービスタイプで索引される処理決定テーブルへのポインタをエントリとして有し、各ポインタは、イベント名および処理実体（例えばプログラム）へのポインタを有する。

【0053】

アクセスリスト111は、外部機器制御部110が外部機器（制御対象となっているネットワーク機器等）の制御を管理するためのトランザクションであり、例えば揮発性メモリ（RAM等）に記憶され、その内容はPNCU1の動作によって動的に変更される。

【0054】

図5は、アクセスリスト111の構成例を示している。アクセスリスト111は、外部機器への設定対象となったユーザ端末のIPアドレス毎にエントリを有する。各エントリは、ユーザ端末のIPアドレス、外部機器への設定情報、状態、外部機器アドレス、およびエントリの有効時間であるタイマを有する。

【0055】

プロトコルライブラリ15は、サービスを提供するために解析が必要なプロトコルのメッセージの型定義とメッセージ解析プログラムにより構成される。プロトコルライブラリ15は、サービス管理テーブル14から参照されるイベント毎の処理実体から参照される。

【0056】

CLIライブラリ112は、ネットワーク機器41～4nに送出するコマンドを定義するキャラクタで構成されるコマンドライン定義文と、コマンドライン定義文に可変パラメータを埋め込んでコマンドラインを編集するコマンドライン編集プログラムと、コマンドを送り込むための通信ライブラリ（例えばTelnet）とを有する。コマンドライン定義文や通信ライブラリは、ネットワーク機器毎に異なるものを持つことができる。

【0057】

初期設定処理部12、PNCU1の起動時に最初に起動されるプログラムであり、提供するサービス機能に応じた初期設定動作を行う。初期設定動作の一例として、アクセス規制サービスを提供する場合にサービス提供対象となるユーザ端末に対するネットワーク機器へのアクセス規制フィルタの設定等がある。

【0058】

図6は、初期設定処理部12の処理の流れを示すフローチャートである。

【0059】

まず、初期設定処理部12は、アドレスリスト11（図3参照）のエントリを1つ読み込む（S1）。続いて、初期設定処理部12は、読み込んだエントリ内のサービスタイプにより索引されるサービス制御テーブル14（図4参照）の処理決定テーブルへのポインタを読み込む（S2）。

【0060】

続いて、初期設定処理部12は、処理決定テーブルをイベント（初期設定）で索引し、該当エントリのポインタが示す処理実体（たとえばプログラム）を実行する（S3）。処理実体の処理はサービス毎に異なる。処理実体の代表的な動作としては、外部機器制御部110を介したネットワーク機器41～4nに対する

アクセス規制フィルタの設定、パケット監視部 13 へのパケット監視条件設定等が挙げられる。

【0061】

処理実体の処理の実行完了後、初期設定処理部 12 は、アドレスリスト 11 の全てのエントリの読み込みが完了したかどうかを判断し (S4)、完了していない場合には、再びステップ S1～S3 の処理を実行し、完了している場合には、パケット監視部 13 を起動した後 (S5)、周期処理部 19 を起動して (S6)、処理を終了する。

【0062】

パケット監視部 13 は、初期設定処理部 12 により起動され、初期設定処理部 12 の初期化動作で設定された条件に従ってパケットの監視を行う。図 7 は、パケット監視部 13 の処理の流れを示すフローチャートである。

【0063】

パケット監視部 13 は、パケット受信待ち状態にあり、受信されるパケットを監視する (S11, S12)。そして、パケット監視部 13 は、パケットを受信すると (S12 で YES)、受信パケットが初期設定処理部 12 により設定されたパケット捕捉条件に一致するかどうかを判断する (S13)。

【0064】

受信パケットがパケット捕捉条件に一致する場合には (S13 で一致)、サービス制御部 16 に受信パケットを与え、サービス制御部 16 を起動する (S14)。一方、受信パケットがパケット捕捉条件に一致しない場合には (S13 で不一致)、パケット監視部 13 は再びパケット受信待ち状態に戻る (S11, S12)。

【0065】

サービス制御部 16 は、パケット監視部 13 により起動され、パケット監視部 13 から通知されたパケット情報に基づき必要なサービス制御を行う。図 8 は、サービス制御部 16 の処理フローを示すフローチャートである。

【0066】

サービス制御部 16 は、パケット監視部 13 から通知された受信パケットの受

信ポート番号に基づいてサービスタイプを決定する（S21）。IPプロトコルでは、通信プロトコル（TCP/UDP等）の受信ポート番号によりサービスを識別することができるので、受信ポート番号に基づいて、サービスタイプが決定される。

【0067】

続いて、サービス制御部16は、受信パケットを、プロトコルライブラリ15を参照して受信パケットのペイロード部に設定されているサービス固有プロトコルを解析し、解析した情報のうちメッセージタイプ（一般にはRequestやReply）に基づいてイベントを決定する。そして、サービス制御部16は、決定されたサービスタイプとイベントによりサービス管理テーブル14を索引する（S22）。

【0068】

続いて、サービス制御部16は、サービス制御データにより索引したエントリが示す処理実体に従い処理を実行する（S23）。処理実体は、例えば、サービスとイベント毎に処理コードが記述されているプログラムであり、サービスとイベントの組み合わせによって処理が異なる。なお、後述の適用例では、いくつかのサービス例を示す。

【0069】

次に、サービス制御部16は、処理実体の処理において、情報をロギングする場合には、ロギング機能部17を起動し、ロギング機能部17にロギング処理を行わせる（S24）。

【0070】

また、サービス制御部16は、処理実体の処理において、他のネットワーク機器、サーバへの情報通知、プロトコル交換等が必要な場合には、通知メッセージ制御部18を起動し、通知メッセージ制御部18にこれらの処理を実行させる（S25）。

【0071】

さらに、サービス制御部16は、処理実体の処理において、ネットワーク機器41～4n（のいずれか）に対して、パケットフィルタの設定等の制御が必要な

場合には、外部機器制御部 110 を起動し、外部機器制御部 110 に該処理を実行させる。

【0072】

ロギング機能部 17 は、PNCU1 の提供サービスの幅を広げるための付加機能であり、捕捉したパケットの様々な情報の中から任意の情報を抽出して、ログメッセージとして編集する機能を有する。ロギング情報編集においては、編集ロジックを容易に組み込むことができるため、通常のプロトコルモニタに比較して特定のサービスに特化したきめ細かなサービスが可能になる。なお、処理の詳細はサービス毎に異なる。

【0073】

通知メッセージ制御部 18 も、PNCU1 の提供サービスの幅を広げるための付加機能であり、捕捉したパケットの特定の情報を他のサービスサーバやネットワーク機器に通知したり、情報の交換を行うための機能を有する。処理の詳細はサービス毎に異なる。

【0074】

ロギング機能部 17 および通知メッセージ制御部 18 は、サービス制御データ 14 から参照される処理実体の処理を容易にするための付加機能であり、これらの機能部以外にも、処理実体間の共通の機能を切り出して新たな機能部を追加することが可能である。

【0075】

外部機器制御部 110 は、サービス制御部 16 により起動され、サービス制御部 16 から通知された情報に基づき、該当するネットワーク機器に対して制御コマンドを送出する。図 9 は、外部機器制御部 110 の処理フローを示すフローチャートである。

【0076】

外部機器制御部 110 は、サービス制御部 16 から通知された情報に基づき、制御すべきネットワーク機器を特定し、サービス制御部 16 から通知された情報と、CLI ライブラリ 112 とを用いて、特定されたネットワーク機器に固有な制御コマンドを編集する (S31)。

【 0 0 7 7 】

続いて、外部機器制御部 1 1 0 は、特定されたネットワーク機器（外部機器）に対して編集したコマンドを、C L I ライブラリ 1 1 2 を用いてネットワーク機器に固有なプロトコル（例えばTelnet）で送信する（S 3 2）。

【 0 0 7 8 】

最後に、外部機器制御部 1 1 0 は、ネットワーク機器へのコマンドの送信（設定）が成功した場合に、設定対象となったユーザ端末の I P アドレス、後に設定情報を変更するために必要となる設定情報、設定状態、情報を設定した外部機器アドレスをアクセスリスト 1 1 1 に登録し（S 3 3）、処理を終了する。

【 0 0 7 9 】

周期処理部 1 9 は、初期設定処理部 1 2 により最初に起動され、以降、周期的にシグナル割り込み等の手法を用いて起動される。周期処理部 1 9 は、アクセスリスト 1 1 1 のエントリに設定されたタイマを管理し、タイマが満了した場合に、サービス制御部 1 6 にタイマ満了イベントを通知する。図 1 0 は、周期処理部 1 9 の処理フローを示すフローチャートである。

【 0 0 8 0 】

周期処理部 1 9 は、アクセスリスト 1 1 1 を読み込み（S 4 1）、アクセスリストエントリに設定されているタイマを減算する（S 4 2）。

【 0 0 8 1 】

続いて、周期処理部 1 9 は、タイマが満了しているかどうかを調べ（S 4 3）、満了している場合には（S 4 3 で Y E S）、アクセスリスト 1 1 1 のエントリに設定されている情報に基づいてタイムアウトイベントを生成し、サービス制御部 1 6 を起動する（S 4 4）。一方、タイマが満了していない場合には、周期処理部 1 9 は、ステップ S 4 4 の処理をスキップする。

【 0 0 8 2 】

続いて、周期処理部 1 9 は、アクセスリスト 1 1 1 の全てのエントリの処理が終了しているかどうかを判断し（S 4 5）、すべてのエントリの処理が終了している場合には、処理を終了し、終了していない場合には、ステップ S 4 1 ～ S 4 4 の処理を繰り返す。

【0083】

次に、PNCU1の利点を示すために、PNCU1をいくつかのサービスに適用した適用例について、それを従来の技術で解決した場合と比較しながら説明する。

【0084】**<第1の適用例>**

第1の適用例として、DHCP (Dynamic Host Configuration Protocol) サーバを利用したネットワークにおいて、PNCU1によりアクセス規制を行うサービス例について説明する。

【0085】

図11は、DHCPサーバによるユーザ端末へのアドレス割り当て（払い出し）を行う場合におけるネットワークのセキュリティ上の問題点の説明図であり、図11（B）は、この問題点を従来技術により解決する場合のネットワークシステムの構成図である。また、図11（C）は、PNCU1によりこの問題点を解決する場合のネットワークシステムの構成図である。

【0086】

PNCU1は、前述したように、図1（A）～（D）のいずれかの構成でネットワークに組み込むことができるが、図11（C）では、一例として図1（C）に示す構成例3による構成のみを示している。

【0087】

図11（A）では、DHCPサーバ2a～2cおよび認証サーバ6が図1（A）～（D）のサービスサーバ2に対応し、L3SW41が図1（A）～（D）のネットワーク機器41に対応する。また、ユーザ端末3aおよび3bが図1（A）～（D）のユーザ端末3に対応する。

【0088】

まず図11（A）を参照して、DHCPサーバ2aを運用しているネットワークでは、通常、ユーザ端末3aのようにDHCPを利用するユーザ端末は、DHCPサーバ2aからIPアドレスやその他の情報を自動的に取得し、ネットワーク4にアクセスする。

【0089】

DHCPサーバ2 aは、一般に、登録されたユーザ端末のみにIPアドレスを割り当てる（払い出す）機能を有する。ネットワークに接続する全てのユーザ端末がDHCPを利用するように設定されていれば、DHCPサーバ2 aに登録されていないユーザ端末には、DHCPサーバ2 aからIPアドレスが払い出されない。したがって、不正にアクセスしようとするユーザ端末は、IPアドレスを取得できず、ネットワークにアクセスできない。

【0090】

しかし、不正にアクセスしようとするユーザ端末3 bが、DHCPサーバ2 aが払い出す情報を何らかの手段で知ることができた場合に、ユーザ端末3 bは、DHCPを利用せずに、IPアドレスやデフォルトルートを直接設定することにより、ネットワークに接続し通信を行うことができる。これは、ユーザ端末が接続したローカルネットワークと外部ネットワークとを接続するネットワーク機器（ここではL3SW41）にDHCPサーバ2 aが払い出したIPアドレスのみを通過させるような規制が設定されていないからである。

【0091】

これを解決する方法としては、図11（B）に示すように、DHCPサーバ、認証サーバ、およびファイアウォール（FW）を組み合わせ、DHCPサーバが払い出したIPアドレスのみを通過可能とする方法が提案されている。

【0092】

まず、DHCPを利用するユーザ端末3 aは、認証サーバ6と通信するための仮のアドレスをDHCPサーバ2 bから取得する。続いて、ユーザ端末3 aは、この仮のアドレスを利用して認証サーバ6にアクセスして認証を受ける。

【0093】

認証後、ユーザ端末3 aは、ネットワークにアクセスして通信するための正規のアドレスの払い出しをDHCPサーバ2 bに要求する。DHCPサーバ2 bは、認証サーバ6と連携しており、アドレス払い出しを要求したユーザ端末3 aが認証済みかどうかを認証サーバ6に確認する。

【0094】

ユーザ端末 3 a が認証済みである場合には、DHCPサーバ 2 b は、FW 7 に対して、ユーザ端末 3 a に払い出す正規のアドレスの規制解除を行うように設定し、ユーザ端末 3 a にこの正規のアドレスを払い出す。

【0095】

一方、DHCPを利用しないユーザ端末 3 b は、DHCPサーバ 2 b によって払い出されたアドレスを有しないので、FW 7 を通過することができず、ネットワークにアクセスして通信を行うことができない。

【0096】

このように、従来の方法により問題を解決する場合には、DHCPサーバ 2 b として、FW 7 の設定を行うことができる特殊なものが必要であり、また、FW 7 も、DHCPサーバ 2 b により設定を受けることができる特殊なものが必要である。したがって、FWを導入することにより、DHCPサーバを特殊なものに交換したり、あるいは、FWと組み合わせて使用できるDHCPサーバに取り替えたりする必要がある。なお、別の方式としては認証サーバとFWが連携する方式もあるが、この場合も認証サーバとして特殊なものが必要となる。したがって、既存の装置をそのまま使用することができない。

【0097】

これに対して、PNCU 1 を利用する場合には、図 11 (C) に示すように、L3SW4 1 にPNCU 1 を接続するだけでアクセス規制を行うことができ、DHCPサーバ 2 c および認証サーバ 5 (ならびにL3SW4 1) は既存のものを使用することができる。

【0098】

図 11 (C) では、FWを使用せず、DHCPサーバ 2 c、認証サーバ 6、およびL3SW4 1 を用いてアクセス規制を行う例を示している。ここで、L3SW4 1 は、設定されたアドレスのパケットのみを通過させる機能を有するものとする。

【0099】

まず、DHCPを利用するユーザ端末 3 a は、認証サーバ 6 と通信するための仮のアドレスをDHCPサーバ 2 c から取得する。続いて、ユーザ端末 3 a は、

この仮のアドレスを使用して認証サーバ6にアクセスし、認証を受ける。

【0100】

認証後、ユーザ端末3aは、DHCPサーバ2cに正規のアドレスの払い出しを要求する。DHCPサーバ2cは認証サーバ6と連携しており、アドレス払い出しを要求したユーザ端末3aが認証済みかどうかを認証サーバ6に確認する。認証済みであれば、DHCPサーバ2cは、ユーザ端末3aに対して正規のアドレスを払い出す。

【0101】

PNCU1は、L3SW41の監視インタフェースに接続され、L3SW41を通過する全てのパケットを監視している。そして、PNCU1は、払い出されたアドレスを含んだ応答メッセージを捕捉すると、応答メッセージを解析する。

【0102】

応答メッセージが正常であり、正規のアドレスを含んでいる場合には、PNCU1は、応答メッセージに含まれる正規のアドレスの規制解除を行うように、L3SW41を設定する。

【0103】

一方、DHCPを利用しないユーザ端末3bは、前述したように、DHCPサーバ2cによってアドレスの払い出しを受けていないので、L3SW41を通過することができず、ネットワークへアクセスすることができない。

【0104】

このように、PNCU1を用いて実現する場合の長所は、特殊なDHCPサーバ、認証サーバ、ファイアウォール等をネットワークに導入することなく、ファイアウォールと同等のアクセス機能を持つネットワーク機器（例えばL3SW）がネットワークに既にあれば、それを利用して、アクセス規制を行うことができることである。さらに、本発明の方式ではDHCPサーバが認証サーバと連携せずにMACアドレス認証等の簡単な認証機能しか持っていない場合にも対応可能である。

【0105】

図11（C）のPNCU1を用いたDHCP手順と連携したアクセス制御につ

いて、以下により具体的に説明する。

【0106】

図12 (A) はアドレスリスト11の一例を、図12 (B) はサービス管理テーブル14の一例を、図12 (C) はアクセスリスト111の一例を、それぞれ示している。

【0107】

PNCU1を起動すると、前述したように、まず初期設定処理部12が起動され、アドレスリスト11が初期設定処理部12に読み込まれる(図6のS1)。

【0108】

アドレスリスト11(図12 (A) 参照) には、サービスタイプとしてDHCPが登録され、サービス固有情報としてDHCPサーバが払い出すIPアドレスの一覧が登録されている。

【0109】

サービスタイプがDHCPであるので、初期設定処理ブロック12は、サービス管理テーブル14(図12 (B) 参照) のDHCP処理決定テーブルをイベント=“初期設定”で索引し(図6のS2)、索引先に示されている処理実体(例えばDHCP_INITで示されるプログラム)を実行する(図6のS3)。

【0110】

図13は、DHCP_INITの処理フローを示すフローチャートである。DHCP_INITの処理では、パケット監視部13のパケット監視条件が設定される(S51)。具体的な設定条件は、UDPパケットの宛先ポート番号67(bootp server)、68(bootp client)である。

【0111】

次に、アドレスリスト11(図12 (A) 参照) のIPアドレス一覧における各IPアドレスに対して、外部機器制御部110が起動されて、初期設定の規制情報が設定される(S52)。設定する情報は、例えばDNS(Domain Name System)、DHCP以外の全てのパケットの規制である。

【0112】

DHCP固有の初期設定処理が終了すると、初期設定処理部12は、パケット

監視部 13 および周期処理部 19 を起動する（図 6 の S 5，S 6）。

【0113】

パケット監視部 13 は、監視インタフェースが受信する全てのパケットを監視し（図 7 の S 11），監視条件に一致するパケットを受信すると、サービス制御部 16 を起動する（図 7 の S 12～S 14）。監視条件は UDP 宛先ポート番号 67，68 である。UDP 宛先ポート番号 67 に一致するものは図 16 のシーケンス図における DHCPDISCOVER と DHCPREQUEST である。UDP 宛先ポート番号 68 に一致するものはシーケンス図における DHCPOFFER と DHCPACK である。

【0114】

サービス制御部 16 は、受信したパケットの UDP 宛先ポート番号が 67 または 68 であることにより、そのパケットが DHCP のメッセージであることを識別する。そして、サービス制御部 16 は、図 18（A）に示すフォーマットを有する DHCP メッセージの DHCP メッセージタイプオプション（図 18（C）参照）を参照してイベントを決定する。

【0115】

メッセージタイプが DHCPACK である場合には、サービス制御部 16 は、イベントをアドレス払い出しに決定する（図 8 の S 21）。また、サービスタイプが DHCP であるので、サービス制御部 16 は、サービス管理テーブル 14（図 12（B）参照）の DHCP 処理決定テーブルをイベント＝“アドレス払い出し”で索引する（図 8 の S 22）。索引先に示されている処理実体（例えばプログラム DHCP_SET）の処理を行う（図 8 の S 23）。

【0116】

図 14 は、DHCP_SET の処理フローを示すフローチャートである。DHCP_SET では、まず、受信した DHCPACK メッセージが解析され、必要情報が抽出される（S 53）。すなわち、DHCP サーバからユーザ端末に払い出された IP アドレスが、図 18（A）の yiaddr フィールドから抽出され、IP アドレスの有効時間が、図 18（B）の IP Address Lease Time フィールドから抽出される。

【0117】

続いて、抽出された IP アドレスおよび有効時間をパラメータにして、外部機

器制御部 110 が起動され、外部機器制御部 110 は、IP アドレスに該当する外部機器（L3SW41）の規制解除を行う（S54）。例えば、IP アドレスに該当する外部機器の全てのプロトコルの規制解除が行われる。

【0118】

外部機器制御部 110 は、DHCP_SET から渡されたパラメータに基づいて、外部機器に設定するコマンドを編集する（図 9 の S31）。続いて、外部機器制御部 110 は、DHCP_SET から渡された IP アドレスのネットワークプレフィックスまたは予め登録されている機器情報に基づき、制御コマンドを送出する外部機器を決定し、外部機器へコマンドが送出手（図 9 の S32）。

【0119】

制御コマンドの設定手順が終了すると、外部機器制御部 110 は、アクセスリスト 111（図 12（C）参照）に設定内容を登録する（図 9 の S33）。具体的には、IP アドレスの欄にユーザ端末の IP アドレスを、状態の欄に「規制無し」を、外部機器アドレスの欄に規制情報を設定した外部機器の IP アドレスを、タイマの欄にアドレスの有効時間を、それぞれ設定する。

【0120】

アドレス返却時には、以下の処理が実行される。

【0121】

パケット監視部 13 のパケットの監視条件は、上記同様に、UDP 宛先ポート番号 67、68 である。図 18 のシーケンス図に示すように、アドレス返却時にユーザ端末から DHCP サーバに送信されるメッセージ DHCPRELEASE は UDP ポート番号 67 を有する。

【0122】

サービス制御部 16 は、受信したパケットが UDP 宛先ポート番号 67 を有することにより、そのパケットが DHCP のメッセージであることを識別し、DHCP メッセージの DHCP メッセージタイプオプション（図 18（C）参照）を参照してイベントを決定する。

【0123】

続いて、サービス制御部 16 は、メッセージタイプが DHCPRELEASE であればイ

ベントをアドレス解放に決定する（図 8 の S 2 1）。サービスタイプが DHCP であるので、サービス制御部 16 は、サービス管理テーブル 14（図 12（B）参照）の DHCP 処理決定テーブルを、イベント＝“アドレス解放”で索引し（図 8 の S 2 2）、索引先に示されている処理実体（例えばプログラム DHCP_REL）の処理を行う（図 8 の S 2 3）。

【0124】

図 15 は、DHCP_REL の処理フローを示すフローチャートである。DHCP_REL では、まず、受信した DHCPRELEASE メッセージが解析され、メッセージから必要な情報が抽出される（S 55）。すなわち、図 18（A）の ciaddr フィールドから、解放する IP アドレスが抽出される。抽出された IP アドレスをパラメータにして、外部機器制御部 110 が起動され、IP アドレスに該当する外部機器の規制解除が行われる（S 56）。初期設定時と同じ規制条件が設定される。

【0125】

外部機器制御部 110 は、DHCP_REL から渡されたパラメータに基づいて、外部機器に設定するコマンドを編集する（図 9 の S 3 1）。また、外部機器制御部 110 は、DHCP_REL から渡された IP アドレスのネットワークプレフィックスまたは予め登録されている機器情報に基づき制御コマンドを送出する外部機器を決定し、外部機器へコマンドを送出する（図 9 の S 3 2）。

【0126】

制御コマンドの設定手順が終了すると、外部機器制御部 110 は、アクセスリスト設定内容を変更する（図 9 の S 3 3）。具体的には、該当する IP アドレスエントリの状態の欄に「規制有り」が設定され、アドレスの有効時間の欄に「無効」が設定される。

【0127】

周期処理部 19 の処理により、アドレスのリリース期間の満了に伴うアクセス規制を設定することもできる。

【0128】

周期処理部 19 は、周期的にアクセスリストを監視し、設定されているタイマを減算する。タイマが満了している場合には、周期処理部 19 は、アクセスリス

ト 1 1 1 のエントリの設定情報に基づいてタイマ満了イベントをサービス制御部 1 6 に通知する（図 1 0 の S 4 1 ～ S 4 4 ）。

【 0 1 2 9 】

サービス制御部 1 6 は、通知されたタイマ満了イベントにより、サービスタイプ＝“DHCP”，イベント＝“タイムアウト”を決定する（図 8 の S 2 1 ）。そして、サービス制御部 1 6 は、サービスタイプが DHCP であるので、サービス管理テーブル 5 4 の DHCP 処理決定テーブルをイベント＝“タイムアウト”で索引し（図 8 の S 2 2 ），索引先に示されている処理実体（例えばプログラム DHCP_REL）の処理を行う（図 8 の S 2 3 ）。

【 0 1 3 0 】

以降の処理は、情報を DHCPRELEASE メッセージではなく、内部イベント情報（タイマ満了イベント）から抽出する点を除き、上記の DHCPRELEASE メッセージの処理と同様である。

【 0 1 3 1 】

このように、PNCU1 を用いることで、既存のネットワーク資源を変更することなく、DHCP 手順と連携したアクセス規制サービスを行うことができる。

【 0 1 3 2 】

なお、前述したように、PNCU1 は、図 1 （A），（B），または（D）に示す構成でネットワークに接続され、または、DHCPサーバ 2 c に内蔵されてもよい。PNCU1 が DHCPサーバ 2 c に内蔵される場合には、PNCU1 の機能をプログラムにより実現して DHCPサーバ 2 c に格納し、DHCPサーバ 2 c の CPU によりこのプログラムを実行させることもできる。

【 0 1 3 3 】

< 第 2 の適用例 >

第 2 の適用例は、移動通信プロトコル Mobile IPv4 におけるファイアウォール（FW）の packets 通過規制解除に PNCU1 を適用したものである。

【 0 1 3 4 】

図 1 9 （A）は、Mobile IPv4 において FW を設置した場合に発生する問題点の説明図であり、図 1 9 （B）は、この問題点を従来技術により解決する場合の

ネットワークシステムの構成図である。また、図 1 9 (C) は、PNCU 1 によりこの問題点を解決する場合のネットワークシステムの構成図である。

【0 1 3 5】

PNCU 1 は、図 1 (A) ~ (D) のいずれかの構成でネットワークに組み込むことができるが、図 1 9 (C) では、一例として図 1 (C) に示す構成例 3 による構成のみを示している。

【0 1 3 6】

図 1 9 (A) ~ (C) において、ユーザ端末 3 は、移動端末（携帯電話等）であり、ホームエージェント（HA：Home Agent）8 のホームネットワークのアドレスをホームアドレスとして有する。ルータ 4 2 は、外部ネットワーク（Foreign Network）に配置されたネットワーク機器であり、外部エージェント（FA：Foreign Agent）であってもよい。ルータ 4 2 とネットワーク 4 との間には、ファイアウォール（FW）7 a または 7 b が接続されている。ユーザ端末 3 は、ホームネットワークから外部ネットワークに移動している。

【0 1 3 7】

図 1 9 (A) において、FW 7 a は、ルータ 4 2 からネットワーク 4 に向けて（すなわち外部ネットワークからネットワーク 4 に向けて）送信されるパケットの送信元アドレスをチェックし、その送信元アドレスが外部ネットワーク内に本来存在しないアドレスである場合には、そのパケットを通過させないように設定されることがある。

【0 1 3 8】

ユーザ端末 3 は、ホームアドレスと外部ネットワークで取得する気付アドレス（Care-of Address）とを保持する。ユーザ端末 3 が、ホームアドレスと気付アドレスとの対応を HA 8 に登録するときは、気付アドレスを用いて通信が行われる一方、ユーザ端末 3 が電子メール等の通常のデータパケットを送信するときは、IP パケットの始点アドレスがホームアドレスに設定される。

【0 1 3 9】

したがって、前述のような FW の設定が行われていると、アドレスの対応を HA 8 に登録する際に送信されるパケットは FW 7 a を通過することができる一方

、通常のデータベースパケットはFW7aを通過することができず、ユーザ端末3は相手端末と通信を行うことができないという問題が発生する。

【0140】

この問題を解決するために、ユーザ端末3が送信するIPパケットを気付アドレスでカプセル化したり、FW7aの設定を動的に変えたりする方法が提案されている。

【0141】

図19(B)は、従来技術による問題の解決方法として、FW7bの設定を動的に変える方法を示している。FW7bは、通過するパケットを監視し、Mobile IPv4の位置登録応答メッセージであるRegistration Replyメッセージを捕捉し、このメッセージ内の結果コードとホームアドレスとを参照して、結果が正常終了であれば、ホームアドレスのアクセス規制を解除する設定を行う。

【0142】

また、他の実現手段としては、認証サーバと連携して認証サーバがFWの穴あけを行う方式もある。

【0143】

いずれの方法でも、特殊なファイアウォールか、特定の認証サーバとファイアウォールの組み合わせをネットワークに設置する必要がある、これまでMobile IPv4を適用していなかったネットワークでは、ネットワーク構成の変更無しではファイアウォール通過のための機能を追加できないこととなる。

【0144】

これに対して、PNCU1を利用する場合には、図19(C)に示すように、ルータ42にPNCU1を接続するだけで、ファイアウォール通過の問題点を解決することができ、FWとして特殊なものを使用する必要もなく、ネットワークの構成を変更する必要もない。

【0145】

図19(C)では、PNCU1は、ルータ42を通過するパケット(Mobile IPv4のメッセージ)を監視し、ユーザ端末3のホームアドレスを取得する。そして、PNCU1は、ユーザ端末3のホームアドレスを有するパケットを通過させ

るようにFW7 aを制御する。

【0 1 4 6】

したがって、PNCU1を利用することにより、FW7 aを特殊なものに取り替える必要もなく、またネットワーク構成を変える必要もない。

【0 1 4 7】

図19 (C) に示すPNCU1を用いたMobile IPv4のファイアウォール通過問題の解決方法について、以下に、より具体的に説明する。

【0 1 4 8】

図20 (A) はアドレスリスト11の一例を、図20 (B) はサービス管理テーブル14の一例を、図20 (C) はアクセスリスト111の一例を、それぞれ示している。

【0 1 4 9】

PNCU1を起動すると、前述したように、まず初期設定処理部12が起動され、アドレスリスト11が読み込まれる(図6のS1)。アドレスリスト11(図20 (A) 参照) には、サービスタイプとしてMobileIPv4が登録されている。サービス固有情報は存在しない。サービスタイプがMobileIPv4であるので、初期設定処理部12は、サービス管理テーブル14のMobile IPv4 処理決定テーブルをイベント＝“初期設定”で索引する(図6のS2)。

【0 1 5 0】

続いて、初期設定処理部12は、索引先に示されている処理実体(たとえばプログラムMobileIP_INIT)の処理を行う(図6のS3)。

【0 1 5 1】

図21は、MobileIP_INITの処理フローを示すフローチャートである。MobileIP_INITでは、パケット監視部13がパケットを監視するための条件が設定される(S61)。具体的な設定条件は、UDPパケットの送信元と宛先ポート番号434 (Mobile IPv4) である。

【0 1 5 2】

MobileIPの初期設定処理を終了すると、初期設定処理部12は、パケット監視部13および周期処理部19を起動する(図6のS5, S6)。

【 0 1 5 3 】

パケット監視部 1 3 は、監視インタフェースにより受信される全てのパケットを監視し（図 7 の S 1 1 ），監視条件に一致するパケットを受信すると、サービス制御部 1 6 を起動する（図 7 の S 1 2 ～ S 1 4 ）。監視条件は U D P 送信元と宛先ポート番号 4 3 4 である。宛先ポート番号 4 3 4 に一致するパケットは、図 2 4 に示す Mobile IPv4 の位置登録シーケンス図における Registration Request であり、送信元ポート番号 4 3 4 に一致するパケットは Registration Reply である。

【 0 1 5 4 】

サービス制御部 1 6 は、受信パケットの U D P 送信元、宛先ポート番号 4 3 4 より、受信パケットが Mobile IP のメッセージであることを識別し、Mobile IPv4 メッセージのメッセージタイプ（Type）（図 2 5 （A）および（B）参照）を参照してイベントを決定する。

【 0 1 5 5 】

メッセージタイプが Registration Reply である場合には、サービス制御部 1 6 は、イベントを位置登録応答に決定する（図 8 の S 2 1 ）。サービスタイプは Mobile IPv4 であるので、サービス制御部 1 6 は、サービス管理テーブル 1 4 （図 2 0 （B）参照）の Mobile IPv4 処理決定テーブルをイベント＝“位置登録応答”で索引する（図 8 の S 2 2 ）。続いて、サービス制御部 1 6 は、索引先に示されている処理実体（例えばプログラム MobileIP_REP）の処理を行う（図 8 の S 2 3 ）。

【 0 1 5 6 】

図 2 2 は、MobileIP_REP の処理フローを示すフローチャートである。MobileIP_REP では、まず、受信した Registration Reply メッセージが解析され、必要な情報が抽出される（S 6 2 ）。

【 0 1 5 7 】

すなわち、位置登録の処理結果が図 2 5 （B）の Code フィールドから抽出され、規制を解除する端末の I P アドレスが図 2 5 （B）の Home Address フィールドから抽出される。また、位置登録の有効時間が図 2 5 （B）の Lifetime フィールド

ドから抽出される。

【0 1 5 8】

Codeフィールドの値が正常応答を示す値（すなわち 0）である場合には（S 6 3 で 0），外部機器制御部 1 1 0 が起動され，I P アドレスに対応する外部機器の規制解除が行われる（S 6 4）。一方，Codeフィールドの値が正常応答を示す値（すなわち 0）でない場合には（S 6 3 で ≠ 0），処理は終了する。

【0 1 5 9】

抽出された I P アドレスと有効時間をパラメータにして，設定される情報は，例えば I P アドレスに対する全てのプロトコルの規制解除である。

【0 1 6 0】

外部機器制御部 1 1 0 は，MobileIP_REPより渡されたパラメータから，外部機器に設定するコマンドを編集する（図 9 の S 3 1）。続いて，外部機器制御部 1 1 0 は，予め登録されている機器情報に基づいて，制御コマンドを送出する外部機器を決定し，外部機器へコマンドを送出する（図 9 の S 3 2）。

【0 1 6 1】

制御コマンドの設定手順が終了すると，アクセスリスト 1 1 1 に設定内容を登録する（図 9 の S 3 3）。具体的には，I P アドレスの欄にユーザ端末の I P アドレスが設定され，状態の欄に規制無しが設定される。また，外部機器アドレスの欄に，規制情報を設定した外部機器の I P アドレスが設定され，タイマにアドレスの有効時間が設定される。

【0 1 6 2】

Mobile IPの明示的な終了手順は，図 2 4 に示す位置登録シーケンス図において，Registration RequestメッセージのLifetimeフィールド（図 2 5 （A）参照）を 0 に設定したメッセージを送信することにより行われる。

【0 1 6 3】

サービス制御部 1 6 は，受信パケットのUDP送信元，宛先ポート番号 4 3 4 より，受信パケットがMobile IPのメッセージであることを識別し，Mobile IPv4メッセージのメッセージタイプを参照してイベントを決定する。

【0 1 6 4】

メッセージタイプがRegistration Requestであれば、サービス制御部 1 6 はイベントが位置登録要求であると判断する（図 8 の S 2 1）。サービスタイプはMobile IPv4であるので、サービス制御部 1 6 は、サービス管理テーブル 1 4（図 2 0（B）参照）のMobile IPv4処理決定テーブルをイベント＝“位置登録要求”で索引する（図 8 の S 2 2）。

【0 1 6 5】

続いて、サービス制御部 1 6 は、索引先に示されている処理実体（例えばプログラムMobileIP_REQ）の処理を行う（図 8 の S 2 3）。

【0 1 6 6】

図 2 3 は、MobileIP_REQの処理フローを示すフローチャートである。MobileIP_REQでは、まず、受信したRegistration Requestメッセージが解析され、対象とするユーザ端末の I P アドレスがHome Addressフィールドから抽出され、位置登録の有効時間がLifetimeフィールドから抽出される（S 6 5）。

【0 1 6 7】

有効時間が 0 であるならば（S 6 6 で 0），外部機器制御部 1 1 0 が起動され，I P アドレスの規制が行われる（S 6 7）。設定する情報は，該当 I P アドレスに対する規制解除条件の解除である。

【0 1 6 8】

外部機器制御部 1 1 0 は，MobileIP_REQから渡されたパラメータに基づいて，外部機器に設定するコマンドを編集する（図 9 の S 3 1）。続いて，外部機器制御部 1 1 0 は，予め登録されている機器情報に基づき，制御コマンドを送出する外部機器を決定し，外部機器へコマンドを送出する（図 9 の S 3 2）。制御コマンドの設定手順が終了すると，外部機器制御部 1 1 0 は，アクセスリスト設定内容を削除する（図 9 の S 3 3）。

【0 1 6 9】

ライフタイム満了に伴うアクセス規制の設定も行われる。周期処理部 1 9 は，周期的にアクセスリスト 1 1 1 を監視し，設定されているタイマを減算する。タイマが満了している場合には，周期処理部 1 9 は，アクセスリスト 1 1 1 のエントリ設定情報に基づいて，タイマ満了イベントをサービス制御部 1 6 に通知する

(図10のS41～S44)。

【0170】

サービス制御部16は、通知されたタイマ満了イベントにより、サービスタイプ＝“MobileIP”，イベント＝“タイムアウト”を決定する(図8のS21)。サービスタイプがMobileIPであるので、サービス制御部16は、サービス管理テーブル14(図24)のMobileIP処理決定テーブルをイベント＝“タイムアウト”で索引する(図8のS22)。索引先に示されている処理実体(例えばプログラムMobileIP_REL)の処理を行う(図8のS23)。

【0171】

以降の処理は、情報を、Registration Requestメッセージではなく、内部イベント情報(タイマ満了イベント)から抽出する点を除き、上記のRegistration Requestメッセージについての処理と同様である。

【0172】

このように、PNCU1を用いることで、特殊なファイアウォールをネットワークに導入することなく、Mobile IPv4を用いるユーザ端末の接続が可能になる。

【0173】

<第3の適用例>

第3の適用例は、IPv6におけるアクセス規制にPNCU1を適用したものである。

【0174】

図26(A)は、IETF(Internet Engineering Task Force)で提案されているIPv6におけるアクセス規制方式の概要を示している。IPv6では、IPv4と同じようにDHCPサーバを用いてアドレスを生成するステートフルアドレス構成方法と、ルータからのネットワークプレフィックスの広告と端末の識別子を組み合わせることでアドレスを自動生成するステートレスアドレス構成方法との2つのアドレス自動構成方法が提案されている。このようなアドレス自動構成では、第1の適用例で示したIPv4のDHCPと同じセキュリティ上の問題が生じる。

【0175】

この解決方法として、アドレス自動生成時に認証手順を絡めることで、認証が成功したユーザ端末のみがネットワークにアクセス可能になるような方式が提案されている。この方式を、ステートレスアドレス自動構成方法を例にとり具体的に説明する。

【0176】

ユーザ端末（IPv6 端末）3 は、ネットワーク機器であるアテンダント（ルータ）43 から広告されたネットワークプレフィックスとユーザ端末3 の識別子とに基づいて IPv6 アドレスを生成する。

【0177】

アドレス生成後、ユーザ端末3 は、生成したアドレスの認証要求をアテンダント43 に送信する。アテンダント43 は、認証サーバ9 との間で交換される認証プロトコルに基づいて、認証要求を認証サーバ9 に転送する。認証サーバ9 は、認証結果をアテンダント43 に返信する。アテンダント43 は、認証結果が認証成功であれば、ユーザ端末3 が提示した IPv6 アドレスのフィルタ規制を解除し、ユーザ端末3 へ認証応答メッセージを返信する。

【0178】

IPv6 で提案されている方式では、アテンダントと呼ばれる特殊なルータが必要となるが、現状このような機能を持ったルータは存在せず、このようなネットワーク構成が広まるにはかなりの時間を要することが予想される。

【0179】

しかし、セキュリティ（アクセス規制）の問題は早急に解決する必要がある。本発明によれば、IPv6 ネットワーク上に、アテンダントと呼ばれる装置の一部の機能を確保し、あるいはそのような機能がない場合でも同様のセキュリティを確保することが可能となる。

【0180】

図26（B）は、アテンダント43 は存在するが、アテンダント43 にアクセス規制を行う機能が無い場合のネットワーク構成例を示すブロック図である。この場合に、PNCU1 は、第1の適用例のDHCPの場合と同様に、認証応答メ

ッセージを捕捉することにより、アテンダント 43 以外の別のアクセス規制機能を持つネットワーク機器（図 26（B）の L3SW41）に対してアクセス規制を設定できる。

【0181】

図 26（C）は、アクセス規制機能を持つネットワーク機器（L3SW41）のみが存在し、アテンダント機能そのものがない場合の例である。この場合に、PNCU1 は、ユーザ端末 3 から送信される認証要求メッセージを捕捉し、ルータ 44 の代わりに、認証サーバ 9 とのメッセージの交換、アクセス規制制御を行う。ユーザ端末 3 からルータ 44 宛てに送信された認証要求メッセージ（オリジナルのメッセージ）はルータ 44 で廃棄される。PNCU1 は、認証処理および規制解除を行った後、ルータ 44 に代わってユーザ端末 3 へ認証応答メッセージを返す。

【0182】

以下に、図 26（C）に示す、PNCU1 を用いた IPv6 アドレス自動構成と連携したアテンダントサービスの具体的な実施例を示す。

【0183】

IPv6 の認証に関する標準技術は、現在のところ確立されていないが、以下では、IETF 草案に基づくステートレスアドレス自動構成を例として説明する。

【0184】

図 27（A）はアドレスリスト 11 の一例を、図 27（B）はサービス管理テーブル 14 の一例を、図 27（C）はアクセスリスト 111 の一例を、それぞれ示している。

【0185】

PNCU1 を起動すると、既に説明したように、まず初期設定処理部 12 が起動され、アドレスリスト 11（図 27（A）参照）が読み込まれる（図 6 の S1）。アドレスリスト 11 には、サービスタイプとして IPv6 が登録されている。なお、アドレスリスト 11 にサービス固有情報は設けられていない。

【0186】

サービスタイプが I P v 6 であるので、初期設定処理部 1 2 は、サービス管理テーブル 1 4（図 2 7（B）参照）の I P v 6 処理決定テーブルをイベント＝“初期設定”で索引する（図 6 の S 2）。続いて、初期設定処理部 1 2 は、索引先に示されている処理実体（例えばプログラム IPV6_INIT）の処理を行う（図 6 の S 3）。

【0 1 8 7】

図 2 8 は、IPV6_INIT の処理フローを示すフローチャートである。IPV6_INIT では、パケット監視部 1 3 のパケット監視条件が設定される（S 7 1）。具体的な設定条件は、ヘッダタイプ（プロトコル）＝I C M P である。

【0 1 8 8】

I P v 6 固有の初期設定処理が終了すると、パケット監視部 1 3 および周期処理部 1 9 が起動される（図 6 の S 5，S 6）。

【0 1 8 9】

パケット監視部 1 3 は、監視インタフェースにより受信される全てのパケットを監視し（図 7 の S 1 1），条件に一致するパケットが受信されると、サービス制御部 1 6 を起動する（図 7 の S 1 2～S 1 4）。

【0 1 9 0】

図 3 1 は、I P v 6 の認証シーケンス図であり、この図に示す I C M P メッセージは全て監視条件に一致する。

【0 1 9 1】

サービス制御部 1 6 は、受信パケットが I P v 6 メッセージであることを識別し、図 3 2 に示す I C M P AAA メッセージのパケット構成におけるメッセージタイプを参照してイベントを決定する。

【0 1 9 2】

メッセージタイプが AAA Request である場合には、サービス制御部 1 6 は、イベントをアドレス払い出しに決定する（図 8 の S 2 1）。サービスタイプは I P v 6 であるので、サービス制御部 1 6 は、サービス管理テーブル 1 4（図 2 7（B）参照）の I P v 6 処理決定テーブルをイベント＝“アドレス払い出し”で索引し（図 8 の S 2 2），索引先に示されている処理実体（例えばプログラム IPV

6_SET) の処理を行う (図 8 の S 2 3) 。

【 0 1 9 3 】

図 2 9 は、IPV 6_SET の処理フローを示すフローチャートである。IPV 6_SET では、まず、認証サーバ (A A A : Authentication, Authorization and Accounting) 9 による該当ユーザの認証を受けるために、ICMP AAA Request メッセージの各パラメータが A A A プロトコルのパラメータに変換され (S 7 2) , 認証サーバ 9 に認証要求が行われる (S 7 3) 。

【 0 1 9 4 】

続いて、認証応答メッセージの結果コードが判定され (S 7 4) , 認証成功であれば (S 7 4 で認証 O K) , 抽出された I P アドレスと有効時間をパラメータにして、外部機器制御部 1 1 0 が起動され、I P アドレスの規制解除が行われる (S 7 5) 。設定される情報は、例えば該当 I P アドレスに対する全てのプロトコルの規制解除である。

【 0 1 9 5 】

外部機器制御部 1 1 0 は、IPV 6_SET より渡されたパラメータから、外部機器に設定するコマンドを編集する (図 9 の S 3 1) 。続いて、外部機器制御部 1 1 0 は、予め登録されている機器情報に基づき、制御コマンドを送出する外部機器を決定し、外部機器へコマンドを送出する (図 9 の S 3 2) 。

【 0 1 9 6 】

続いて、外部機器制御部 1 1 0 は、制御コマンドの設定手順が終了すると、アクセスリスト 1 1 1 に設定内容を登録する (図 9 の S 3 3) 。具体的には、I P アドレスの欄に端末の I P アドレスを、状態の欄に規制無しを、外部機器アドレスの欄に、規制情報を設定した外部機器の I P アドレスを、タイマの欄にアドレスの有効時間を、それぞれ設定する。

【 0 1 9 7 】

最後に、ICMP AAA Reply メッセージが編集され、該当端末へ送信される (S 7 6) 。

【 0 1 9 8 】

図 3 3 は、I P v 6 の明示的な終了シーケンスを示している。サービス制御部

16は、受信したICMPパケットより、ICMP AAAメッセージのメッセージタイプを参照してイベントを決定する。メッセージタイプがAAA Teardownであれば、サービス制御部16は、イベントをアドレス解放に決定する(図8のS21)。サービスタイプがIPv6であるので、サービス管理テーブル14(図27(B)参照)のIPv6処理決定テーブルをイベント=“アドレス解放”で索引し(図8のS22)、索引先に示されている処理実体(例えばプログラムIPV6_REL)の処理を行う(図8のS23)。

【0199】

図30は、IPV6_RELの処理フローを示すフローチャートである。IPV6_RELでは、まず、受信したAAA TeardownメッセージのパラメータがAAAプロトコルに変換される(S77)。続いて、セッションが解放される(S78)。

【0200】

続いて、外部機器制御部110が起動され、該当IPアドレスの規制が行われる(S79)。設定する情報は、該当IPアドレスに対する規制解除条件の削除である。

【0201】

外部機器制御部110は、IPV6_RELから渡されたパラメータに基づいて、外部機器に設定するコマンドを編集する(図9のS31)。続いて、外部機器制御部110は、予め登録されている機器情報に基づき、制御コマンドを送出する外部機器を決定し、外部機器へコマンドを送出する(図9のS32)。制御コマンドの設定手順が終了すると、外部機器制御部110は、アクセスリスト111の設定内容を削除する(図9のS33)。

【0202】

最後に、ICMP AAA Replyメッセージが編集され、該当端末へ送信される(図30のS80)。

【0203】

ライフタイム満了に伴うアクセス規制も設定される。周期処理部19は、周期的にアクセスリスト111を監視し、設定されているタイマを減算する。タイマが満了している場合には、周期処理部19は、アクセスリスト111のエントリ

の設定情報をもとに、タイマ満了イベントをサービス制御部 16 に通知する（図 10 の S 4 1 ～ S 4 4 ）。

【0204】

サービス制御部 16 は、通知されたタイマ満了イベントにより、サービスタイプ＝“IPv6”，イベント＝“タイムアウト”を決定する（図 8 の S 2 1）。サービスタイプが IPv6 であるので、サービス制御部 16 は、サービス管理テーブル 14 の IPv6 処理決定テーブルをイベント＝“タイムアウト”で索引し（図 8 の S 2 2），索引先に示されている処理実体（例えばプログラム IPV6_REL）の処理を行う（図 8 の S 2 3）。

【0205】

以降の処理は、情報を ICMP AAA Teardown メッセージではなく、内部イベント情報（タイマ満了イベント）から抽出する点を除き上記と同様である。

【0206】

このように、PNCU1 を用いることで、基本的な IPv6 機能しか有しないネットワークに対して、認証等の付加サービスを容易に追加することができる。

【0207】

（付記 1） ユーザ端末に所定のサービスを提供するサービス装置に代行して、該サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置であって、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と、

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定して実行する実行部と、

を備えている代理ネットワーク制御装置。

【0208】

（付記 2） ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行する代理

ネットワーク制御装置であって、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視するパケット監視部と、

前記パケット監視部により監視されたパケットに基づいて前記補完または拡張する機能を決定するサービス制御部と、

前記サービス制御部により決定された機能に基づいて前記ネットワーク装置を制御する外部機器制御部と、

を備えている代理ネットワーク制御装置。

【0209】

(付記3) 付記2において、

前記サービス装置はD H C Pサーバであり、

前記パケット監視部は、前記サービス装置から前記ユーザ端末に発行されるアドレスを含んだパケットを監視し、

前記サービス制御部は、前記パケット監視部により監視されたパケットに基づいて、前記サービス装置により発行されたアドレスを送信元アドレスとして有するパケットを通過させ、それ以外のアドレスを送信元アドレスとして有するパケットを通過させないアクセス規制機能を決定し、

前記外部機器制御部は、前記アクセス規制機能を実行するように前記ネットワーク装置を制御する、

代理ネットワーク制御装置。

【0210】

(付記4) 付記2において、

前記ユーザ端末がホームネットワークのホームアドレスを有する移動通信端末であり、前記ネットワーク装置が前記ホームネットワークの外部ネットワークから外部に送信されるパケットのうち、所定の送信元アドレスを有するパケットを通過させ、それ以外のパケットを通過させないファイアウォールであり、

前記パケット監視部は、前記外部ネットワークに移動した前記ユーザ端末と前記ホームネットワークのホームエージェントとの間で通信される、前記ユーザ端末のホームアドレスを含んだパケットを監視し、

前記サービス制御部は、前記パケット監視部により監視されたパケットに基づいて、前記ホームアドレスを有するパケットを通過させるようにアクセス規制を解除する機能を決定し、

前記外部機器制御部は、前記アクセス規制を解除する機能を実行するように、前記ネットワーク装置を制御する、

代理ネットワーク制御装置。

【0 2 1 1】

(付記 5) 付記 2 において、

前記ユーザ端末が I P v 6 端末であり、前記サービス装置が生成された前記ユーザ端末の I P アドレスの認証を行う認証サーバであり、

前記パケット監視部は、前記サービス装置により認証された I P アドレスを含むパケットを監視し、

前記サービス制御部は、前記パケット監視部により監視されたパケットに基づいて、前記 I P アドレスを送信元アドレスとして有するパケットを通過させるようにアクセス規制を解除する機能を決定し、

前記外部機器制御部は、前記アクセス規制を解除する機能を実行するように、前記ネットワーク装置を制御する、

代理ネットワーク制御装置。

【0 2 1 2】

(付記 6) 付記 5 において、

前記ユーザ端末の I P アドレスを生成して前記ユーザ端末に送信し、または、ネットワークプレフィックスを前記ユーザ端末に送信するアドレス送信部をさらに備えている、

代理ネットワーク制御装置。

【0 2 1 3】

(付記 7) 付記 2 において、

前記サービス制御部により決定される前記機能は、所定の情報を記録する機能を含む、

代理ネットワーク制御装置。

【 0 2 1 4 】

(付記 8) 付記 2 において、

前記サービス制御部により決定される前記機能は、所定のネットワーク装置またはサービス装置にメッセージを送信する機能を含む、

代理ネットワーク制御装置。

【 0 2 1 5 】

(付記 9) コンピュータに、

ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間で通信されるパケットを監視する手順と、

前記監視したパケットに基づいて、前記サービス装置に代行して、該サービス装置の機能を補完または拡張する機能を決定して実行する手順と、

を実行させるためのプログラム。

【 0 2 1 6 】

(付記 1 0) ユーザ端末と該ユーザ端末に所定のサービスを提供するサービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を前記サービス装置に代行して実行するコンピュータに、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視する手順と、

前記監視したパケットに基づいて前記補完または拡張する機能を決定する手順と、

前記決定した機能に基づいて前記ネットワーク装置を制御する手順と、
を実行させるためのプログラム。

【 0 2 1 7 】

(付記 1 1) ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し、所定の条件を満たすパケットに基づいて、前記サービス装置の機能を補完または拡張

張する機能を実行する代理ネットワーク制御装置と、
を備えているネットワークシステム。

【 0 2 1 8 】

(付記 1 2) 付記 9 において、
前記代理ネットワーク制御装置は前記サービス装置に内蔵されている、ネットワークシステム。

【 0 2 1 9 】

(付記 1 3) ユーザ端末と通信を行い該ユーザ端末に所定のサービスを提供するサービス装置と、

前記ユーザ端末と前記サービス装置との間に配置されて前記ユーザ端末と前記サービス装置との間で通信されるパケットの転送を行うネットワーク装置と、

前記ユーザ端末と前記サービス装置との間で通信されるパケットを監視し、所定の条件を満たすパケットに基づいて前記ネットワーク装置を制御することにより、前記サービス装置の機能を補完または拡張する機能を実行する代理ネットワーク制御装置と、
を備えているネットワークシステム。

【 0 2 2 0 】

(付記 1 4) 付記 1 3 において、
前記代理ネットワーク制御装置は前記サービス装置に内蔵されている、ネットワークシステム。

【 0 2 2 1 】

(付記 1 5) 付記 1 3 において、
前記サービス装置は D H C P サーバであり、
前記代理ネットワーク制御装置は、前記サービス装置から前記ユーザ端末に配布されるアドレスを含んだパケットを監視し、前記ユーザ端末から送信される、前記アドレスを送信元アドレスとして有するパケットを通過させ、それ以外のパケットを通過させないように前記ネットワーク装置を制御する、
ネットワークシステム。

【 0 2 2 2 】

(付記 1 6) 付記 1 3 において、

前記ユーザ端末がホームネットワークのホームアドレスを有する移動通信端末であり、

前記ネットワーク装置は、前記ホームネットワークの外部ネットワークから外部に送信されるパケットのうち、所定の送信元アドレスを有するパケットを通過させ、それ以外のパケットを通過させないネットワーク装置であり、

前記代理ネットワーク制御装置は、前記外部ネットワークに移動した前記ユーザ端末と前記ホームネットワークのホームエージェントとの間で通信される、前記ユーザ端末のホームアドレスを含んだパケットに基づいて、前記ユーザ端末のホームアドレスを送信元アドレスとして含むパケットを通過させるように前記ネットワーク装置を制御する、

ネットワークシステム。

【 0 2 2 3 】

(付記 1 7) 付記 1 3 において、

前記ユーザ端末が I P v 6 端末であり、前記サービス装置は生成された前記ユーザ端末の I P アドレスの認証を行う認証サーバであり、

前記代理ネットワーク制御装置は、前記サービス装置により認証された I P アドレスを送信元アドレスとして有するパケットを通過させるように前記ネットワーク装置を制御する、

ネットワークシステム。

【 0 2 2 4 】

(付記 1 8) 付記 1 7 において、

前記代理ネットワーク制御装置は、前記ユーザ端末の I P アドレスを生成して前記ユーザ端末に送信し、または、ネットワークプレフィックスを前記ユーザ端末に送信する機能をさらに実行する、

ネットワークシステム。

【 0 2 2 5 】

【発明の効果】

本発明によると、既存のネットワーク構成を変更せずに、新たなネットワーク

サービスの付加機能を追加することができる。

【0 2 2 6】

たとえば、D H C P の運用時に問題となるセキュリティの問題を、より容易に低コストで実現することができる。また、Mobile IPv4においては、外部ネットワークに存在するユーザ端末のデータパケットがファイアウォールを通過できないといった問題を低コストで解決することができる。さらに、I P v 6 のアクセス規制方式に対しても、特殊な装置を導入することなくアクセス規制の機能を提供することができる。

【0 2 2 7】

またさらに、本発明による代理ネットワーク制御装置をネットワークに実装することにより、様々なサービスに対して機能追加が容易となる。

【図面の簡単な説明】

【図 1】

(A) ～ (D) は、本発明の実施の形態による代理ネットワーク制御装置 (P N C U) を有するネットワークシステムの構成例を示すブロック図である。

【図 2】

P N C U の機能ブロック図である。

【図 3】

アドレスリストの構成例を示す。

【図 4】

サービス管理テーブルの構成例を示す。

【図 5】

アクセスリストの構成例を示す。

【図 6】

P N C U の初期設定処理部の処理の流れを示すフローチャートである。

【図 7】

P N C U のパケット監視部の処理の流れを示すフローチャートである。

【図 8】

P N C U のサービス制御部の処理フローを示すフローチャートである。

【図 9】

PNCUの外部機器制御部の処理フローを示すフローチャートである。

【図 1 0】

PNCUの周期処理部の処理フローを示すフローチャートである。

【図 1 1】

(A) は、DHCPサーバによるユーザ端末へのアドレス割り当て（払い出し）を行う場合におけるネットワークのセキュリティ上の問題点の説明図であり、

(B) は、この問題点を従来技術により解決する場合のネットワークの構成図であり、(C) は、PNCUによりこの問題点を解決する場合のネットワークシステムの構成図である。

【図 1 2】

(A) はアドレスリストの一例を、(B) はサービス管理テーブルの一例を、(C) はアクセスリストの一例を、それぞれ示す。

【図 1 3】

DHCP_INITの処理フローを示すフローチャートである。

【図 1 4】

DHCP_SETの処理フローを示すフローチャートである。

【図 1 5】

DHCP_RELの処理フローを示すフローチャートである。

【図 1 6】

DHCPにおけるアドレス払い出し時のメッセージフローを示すシーケンス図である。

【図 1 7】

DHCPにおけるアドレス返却時のメッセージフローを示すシーケンス図である。

【図 1 8】

(A) はDHCPメッセージのフォーマットを示し、(B) および (C) はオプションを示す。

【図 1 9】

(A) は、Mobile IPv4においてF Wを設置した場合に発生する問題点の説明図であり、(B) は、この問題点を従来技術により解決する場合のネットワークシステムの構成図であり、(C) は、P N C Uによりこの問題点を解決する場合のネットワークシステムの構成図である。

【図 2 0】

(A) はアドレスリストの一例を、(B) はサービス管理テーブルの一例を、(C) はアクセスリストの一例を、それぞれ示す。

【図 2 1】

MobileIP_INITの処理フローを示すフローチャートである。

【図 2 2】

MobileIP_REPの処理フローを示すフローチャートである。

【図 2 3】

MobileIP_REQの処理フローを示すフローチャートである。

【図 2 4】

Mobile IPv4の位置登録シーケンス図である。

【図 2 5】

(A) はMobile IPv4のRegistration Requestのパケット構成図であり、(B) はMobile IPv4のRegistration Replyのパケット構成図である。

【図 2 6】

(A) は、I E T Fで提案されているI P v 6におけるアクセス規制方式の概要を示し、(B) および(C) は、P N C Uによりアクセス規制を行う場合のネットワークシステムの構成図である。

【図 2 7】

(A) はアドレスリストの一例を、(B) はサービス管理テーブルの一例を、(C) はアクセスリストの一例を、それぞれ示す。

【図 2 8】

IPV6_INITの処理フローを示すフローチャートである。

【図 2 9】

IPV 6 _SETの処理フローを示すフローチャートである。

【図 3 0】

IPV 6 _REL の処理フローを示すフローチャートである。

【図 3 1】

I P v 6 の認証シーケンス図である。

【図 3 2】

ICMP AAA メッセージのパケット構成を示す。

【図 3 3】

I P v 6 の明示的な終了シーケンスを示す。

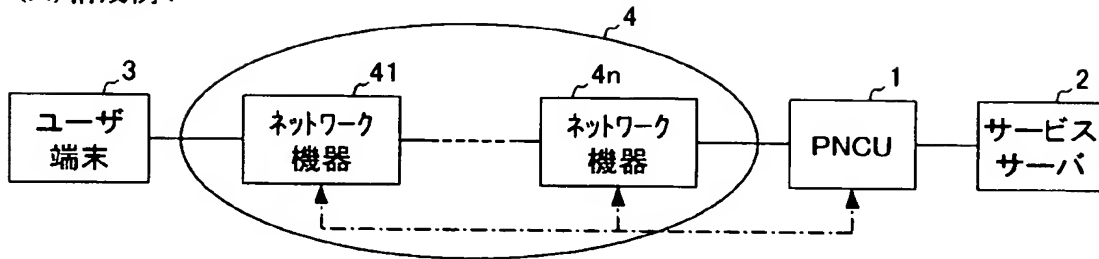
【符号の説明】

- 1 P N C U
- 2 サービスサーバ
- 3 ユーザ端末
- 4 ネットワーク
- 4 1 ～ 4 n ネットワーク機器
- 1 1 アドレスリスト
- 1 2 初期設定処理部
- 1 3 パケット監視部
- 1 4 サービス管理テーブル
- 1 6 サービス制御部
- 1 1 0 外部機器制御部
- 1 1 1 アクセスリスト

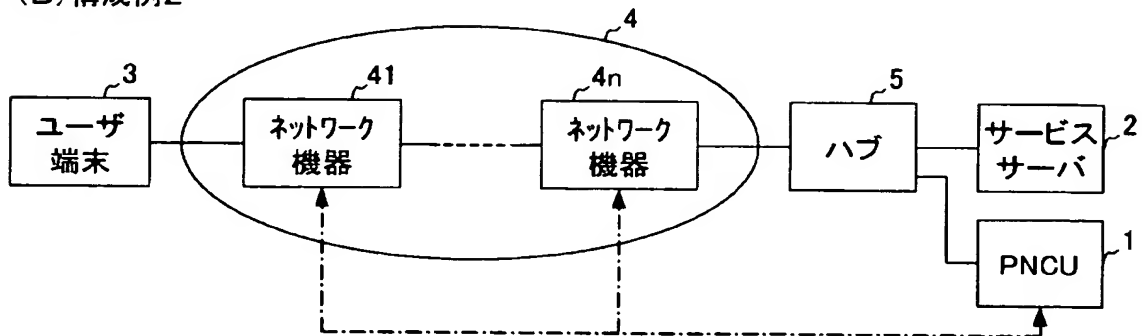
【書類名】 図面

【図 1】

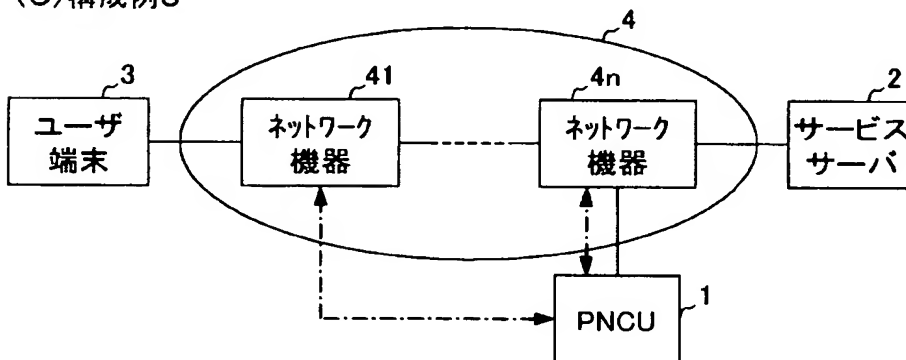
(A) 構成例 1



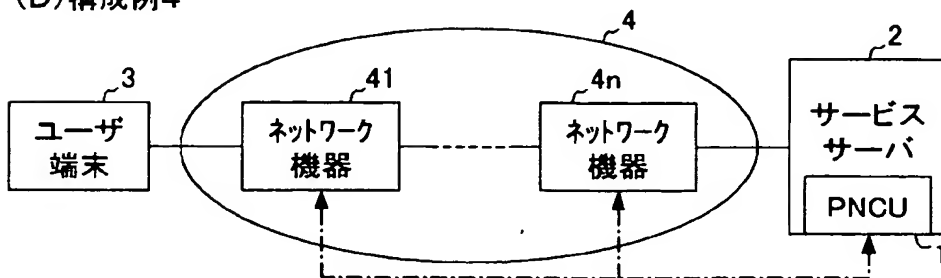
(B) 構成例 2



(C) 構成例 3

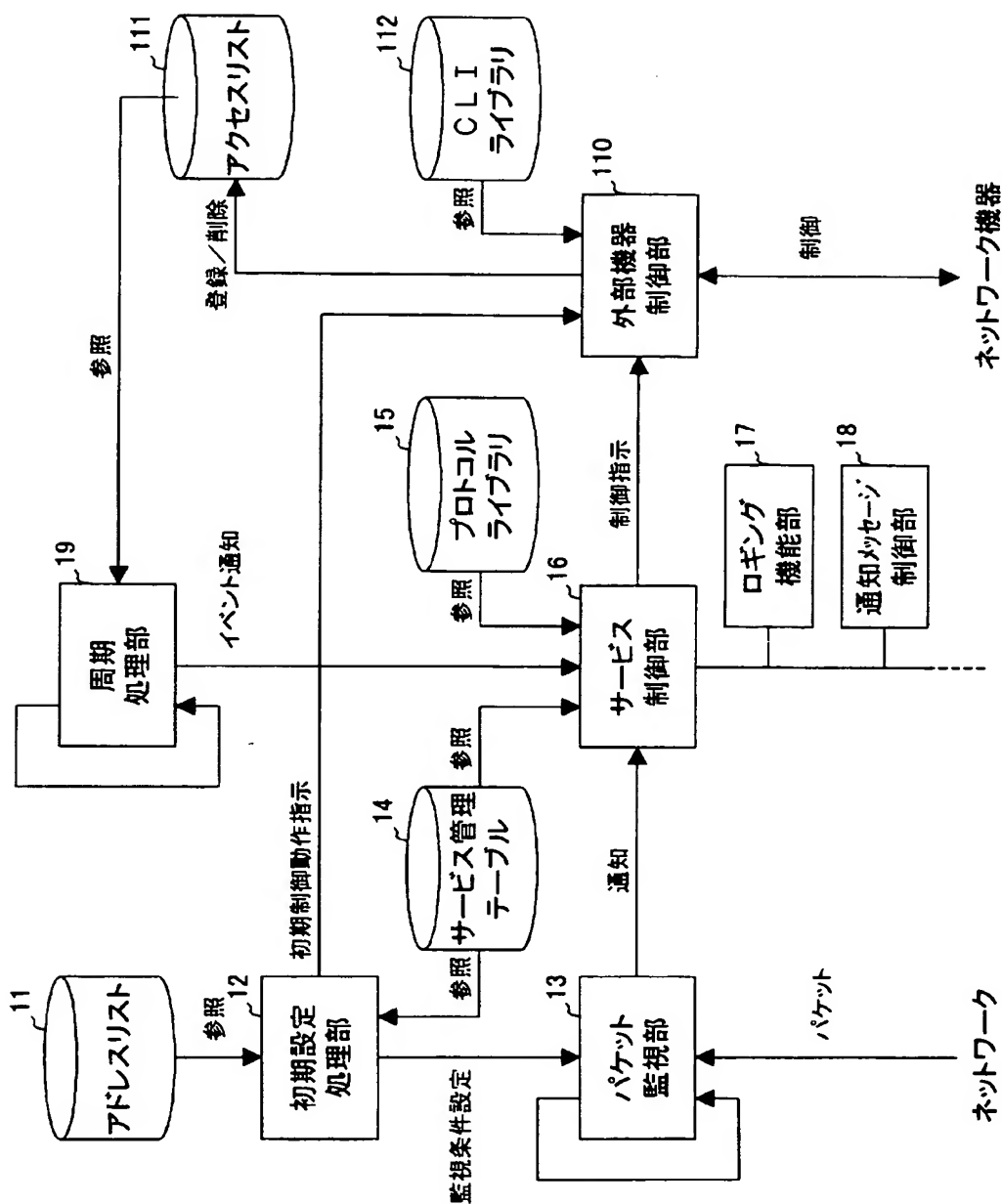


(D) 構成例 4



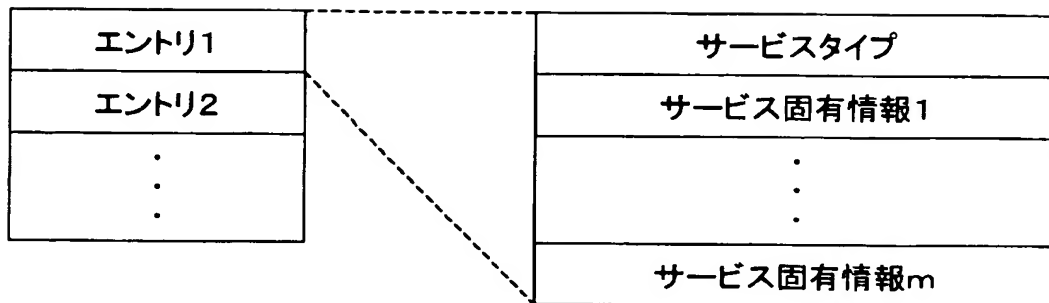
【図 2】

PNCUの構成



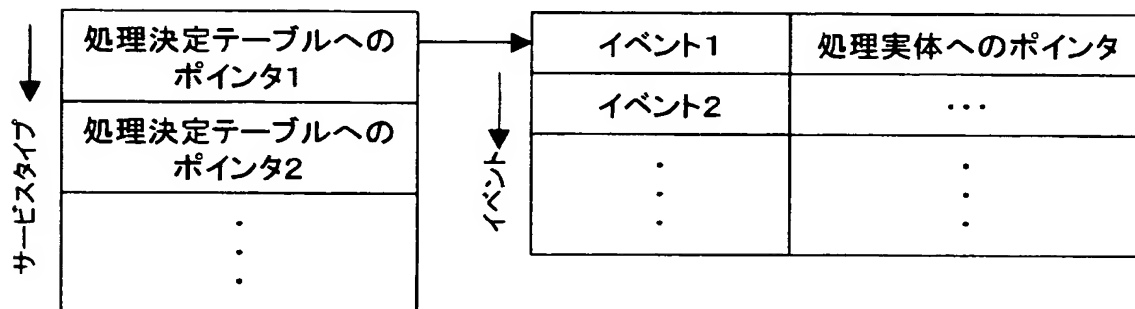
【図 3】

アドレスリスト



【図 4】

サービス管理テーブル

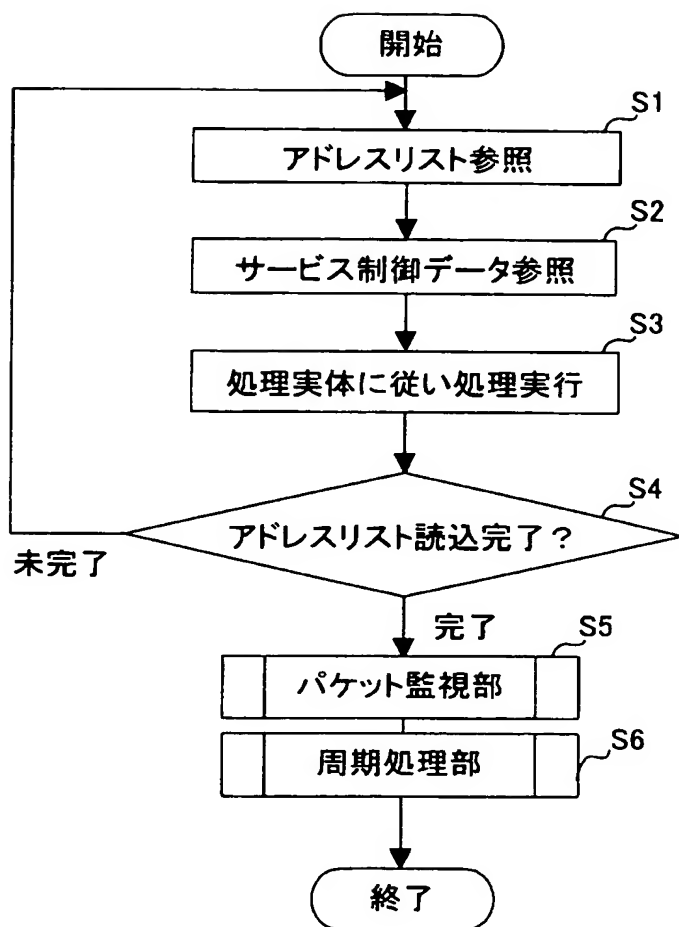


【図 5】

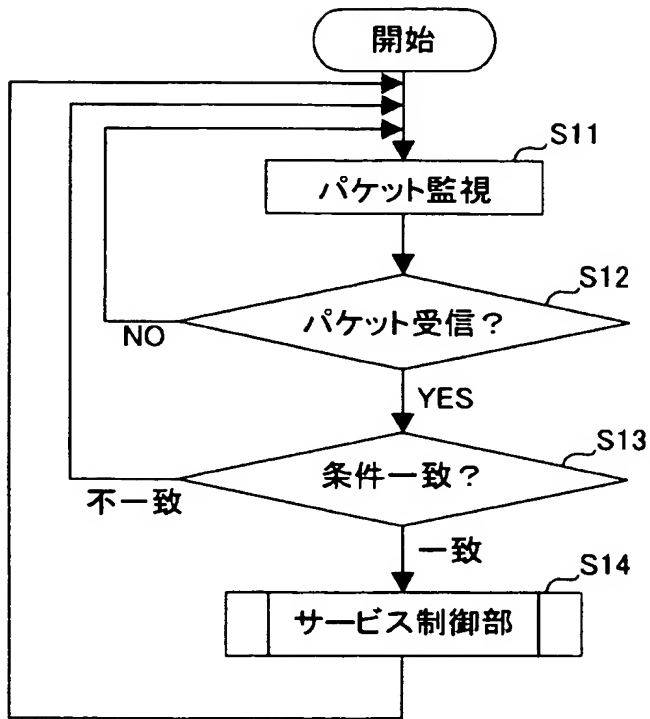
アクセスリスト

IPアドレス	設定情報	状態	外部機器アドレス	タイマ
...
⋮	⋮	⋮	⋮	⋮

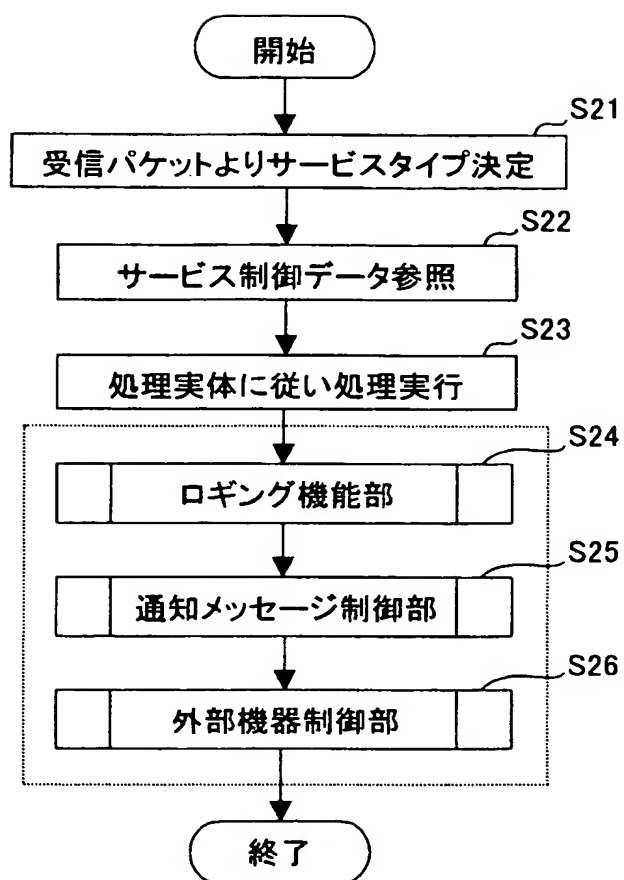
【図 6】



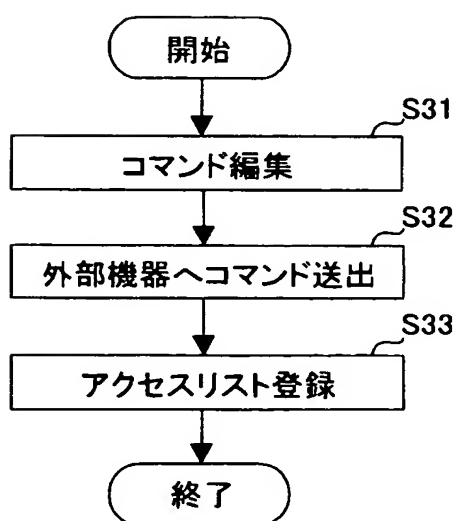
【図 7】



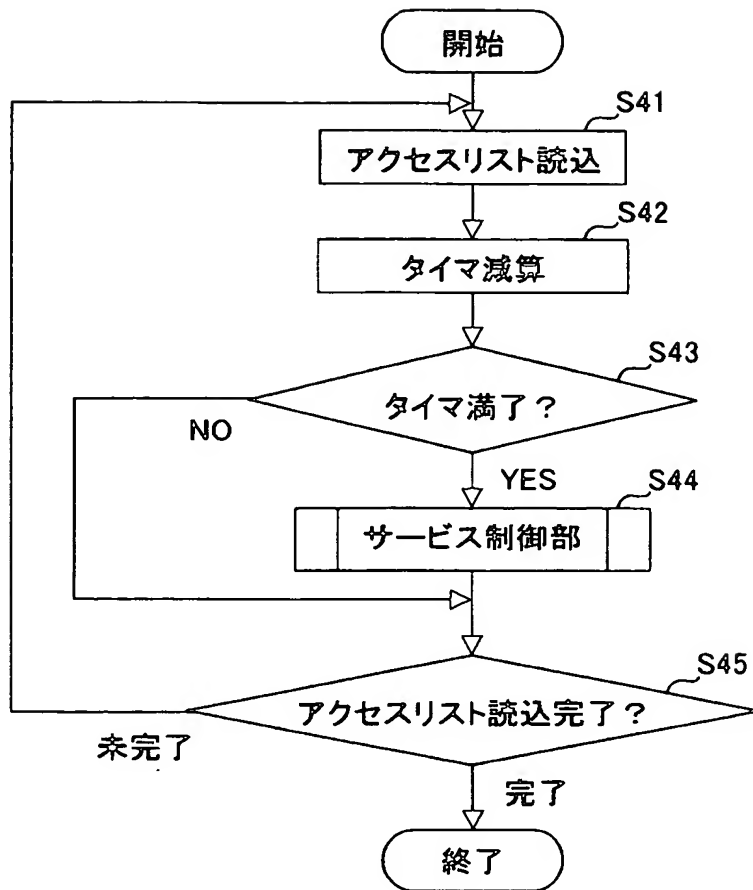
【図 8】



【図 9】

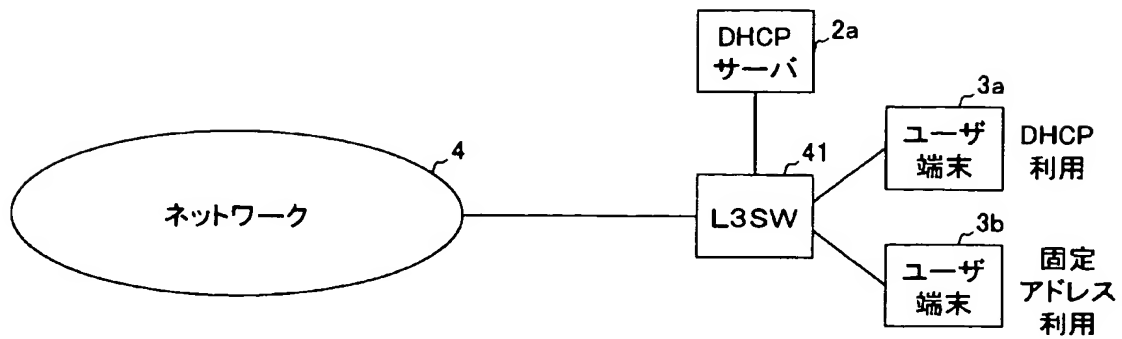


【図10】

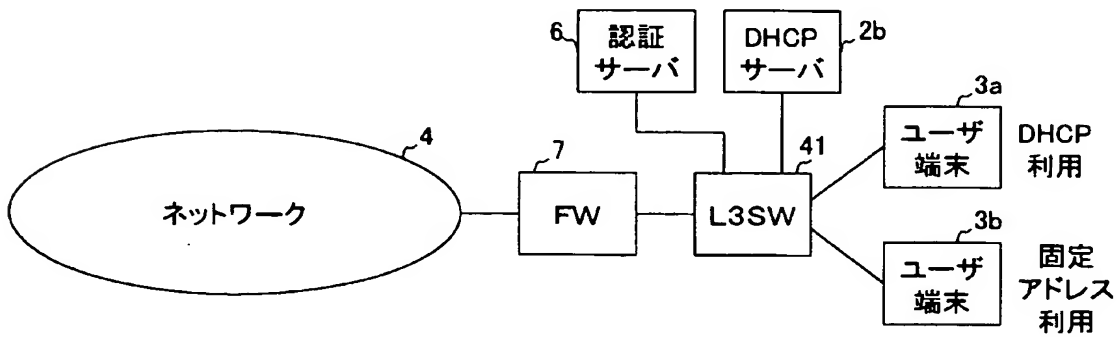


【図 11】

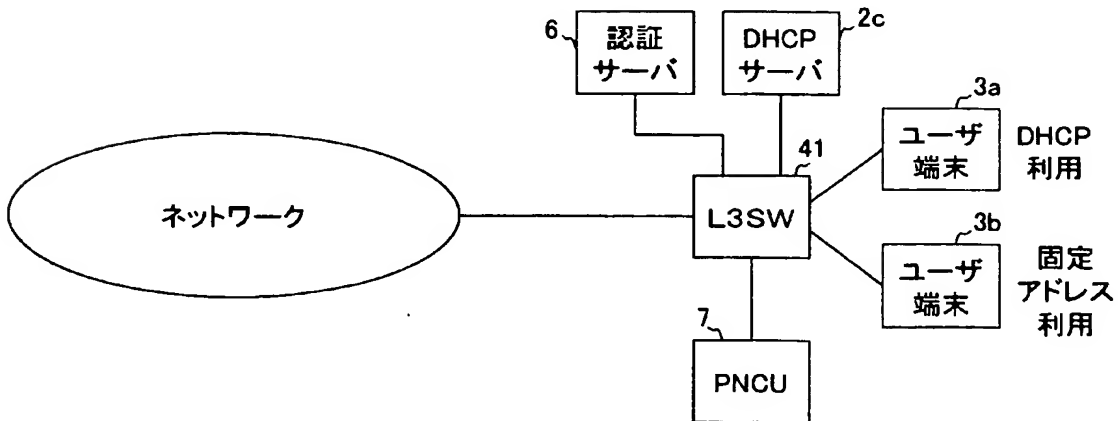
(A) DHCPのセキュリティ上の問題点



(B) 従来技術による解決方法



(C) 本発明の実施の形態による解決方法



【図 12】

(A) アドレスリスト

エントリ1		サービスタイプ: DHCP
エントリ2		サービス固有情報1: 10.115.250.10
⋮		⋮
⋮		サービス固有情報m: 10.115.250.255

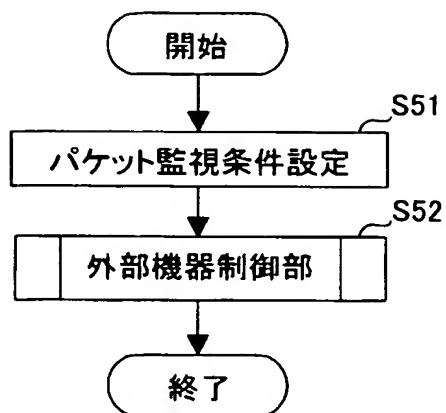
(B) サービス管理テーブル

処理決定テーブルへの ポインタ1		イベント	処理実体へのポインタ
処理決定テーブルへの ポインタ2		初期設定	DHCP_INIT
⋮		アドレス配布	DHCP_SET
⋮		アドレス解放	DHCP_REL
⋮		タイムアウト	DHCP_TO

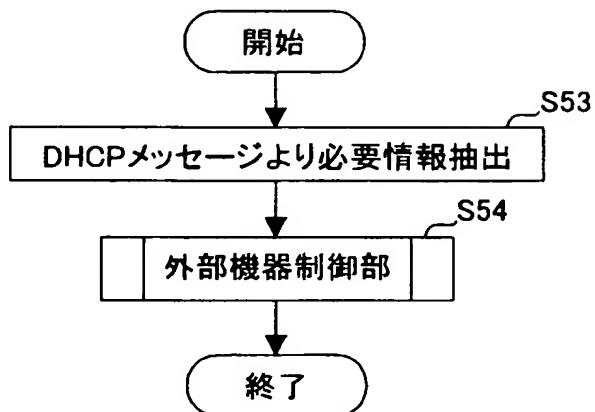
(C) アクセスリスト

IPアドレス	設定情報	状態	外部機器アドレス	タイマ
10.115.250.10	...	規制有り	10.115.250.1	8H
10.115.250.11	...	規制無し	10.115.250.1	...
⋮	⋮	⋮	⋮	⋮

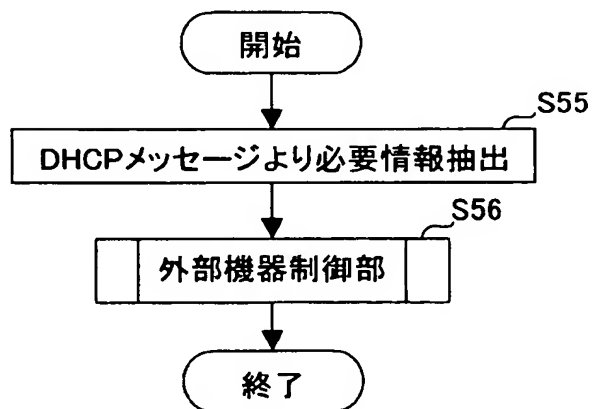
【図 13】



【図 14】

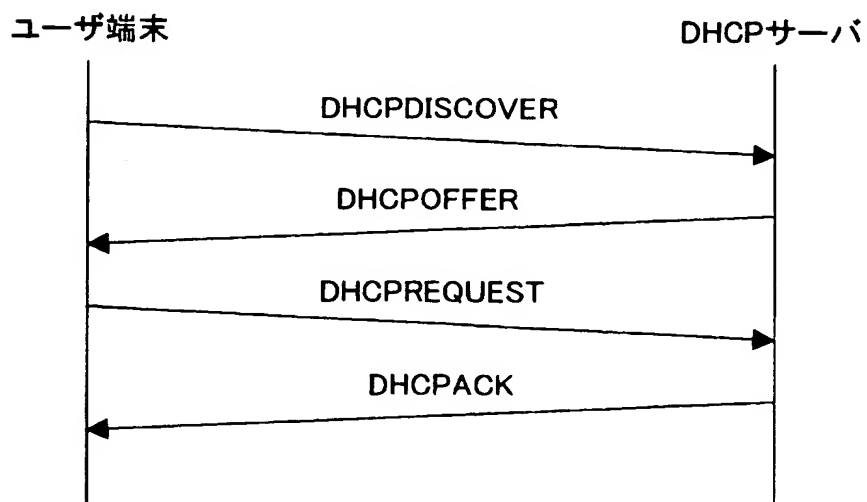


【図 15】



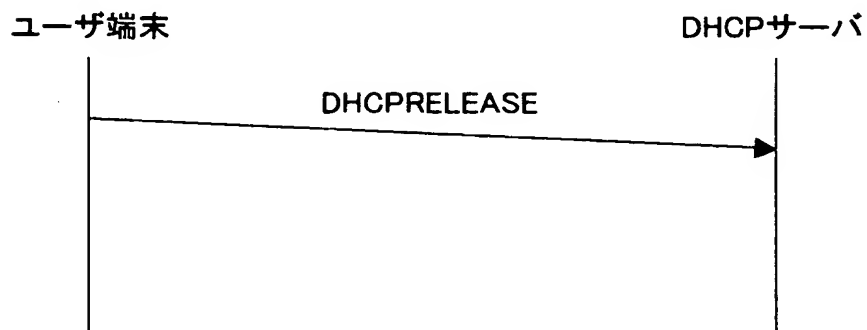
【図 16】

DHCPサーバのアドレス配布シーケンス



【図 17】

DHCPサーバのアドレス解放シーケンス



【図 1 8】

(A) DHCPメッセージフォーマット

0									1									2									3								
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0					
op(1)									htype(1)									hlen(1)									hops(1)								
xid(4)																																			
secs(2)																flags(2)																			
ciaddr(4)																																			
yiaddr(4)																																			
siaddr(4)																																			
giaddr(4)																																			
chaddr(16)																																			
sname(64)																																			
file(128)																																			
options(variable)																																			

(B) IP Address Lease Timeオプション

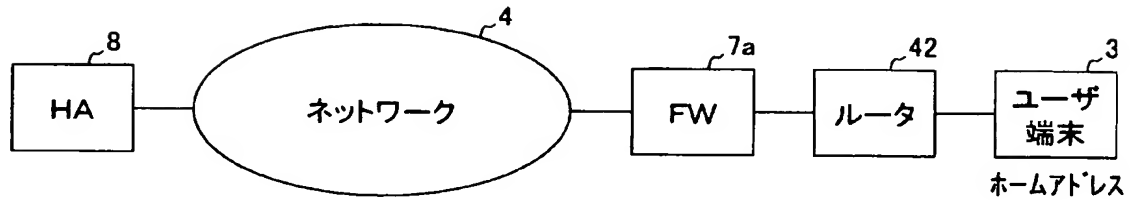
Code	Len		Lease Time			
51	4	t1	t2	t3	t4	

(C) DHCP Message Typeオプション

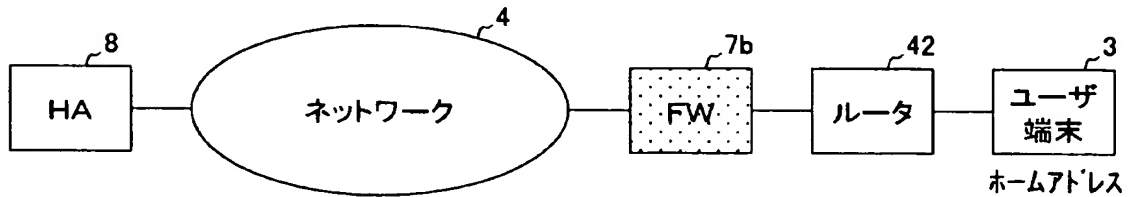
Code	Len	Type
53	1	1-9

【図 19】

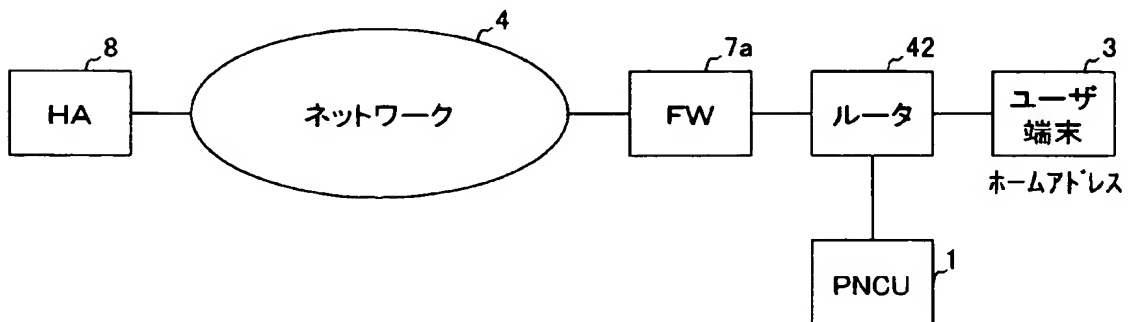
(A) Mobile IPv4のファイアウォール通過問題



(B) 従来技術による解決方法



(C) 本発明の実施の形態による解決方法

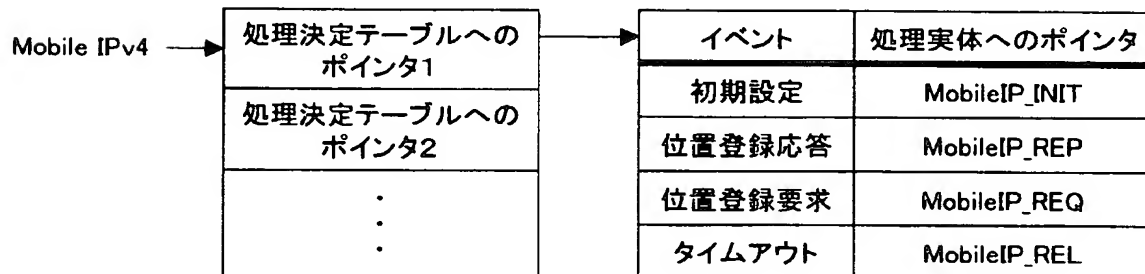


【図 20】

(A) アドレスリスト

エントリ1		サービスタイプ: Mobile IPv4
エントリ2		
⋮		

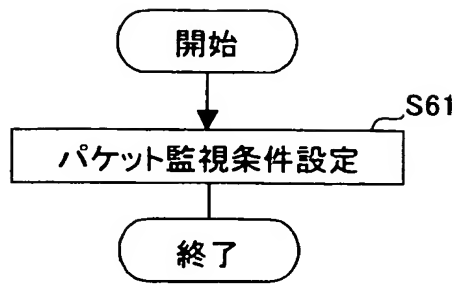
(B) サービス管理テーブル



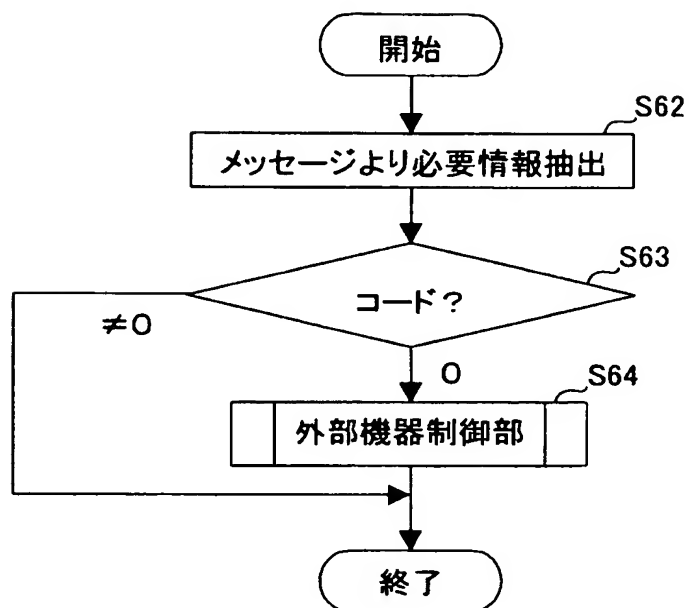
(C) アクセスリスト

IPアドレス	設定情報	状態	外部機器アドレス	タイマ
10.115.10.10	...	規制無し	10.115.250.1	8H
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮

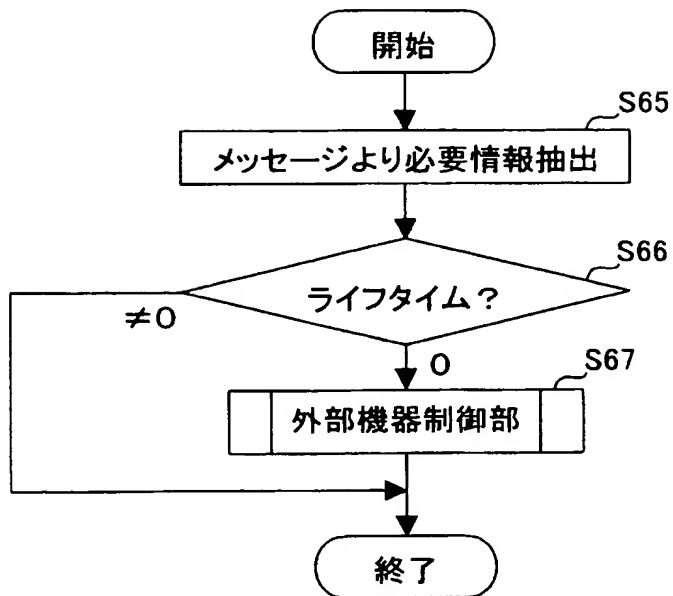
【図 21】



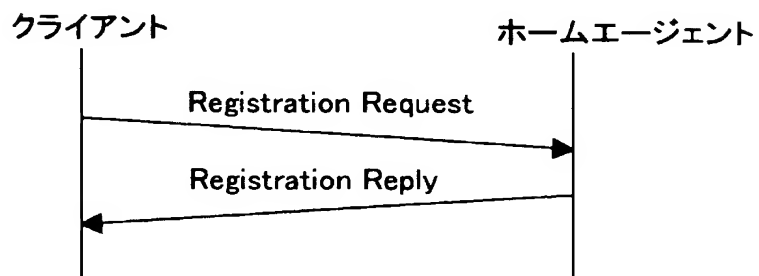
【図 22】



【図 23】



【図 24】



【図 2 5】

(A) Registration Request

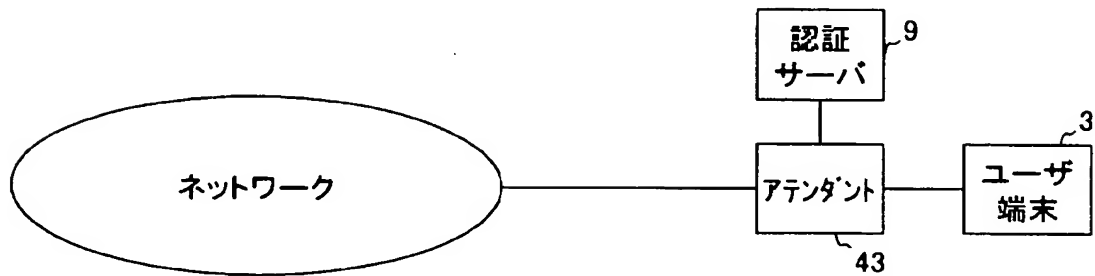
0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Type								S	B	D	M	G	V	rsv		Lifetime																							
Home Address																																							
Home Agent																																							
Care-of Address																																							
Identification																																							
Extensions ...																																							

(B) Registration Reply

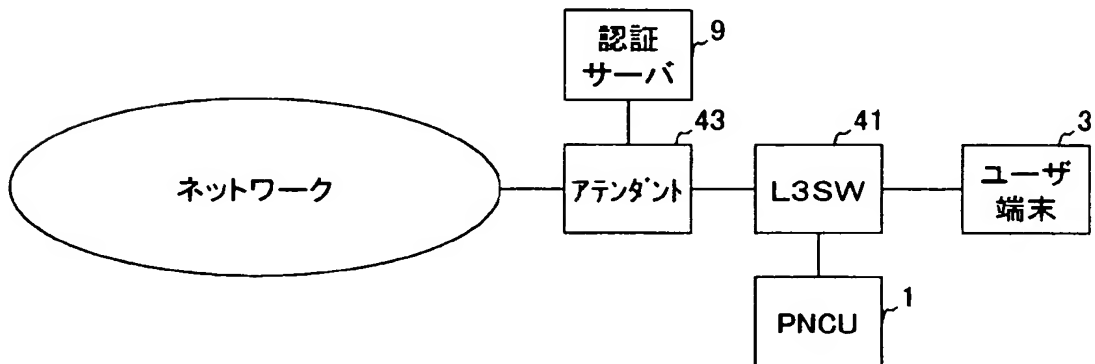
0	1									2									3																
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1				
Type									Code									Lifetime																	
Home Address																																			
Home Agent																																			
Identification																																			
Extensions ...																																			

【図 26】

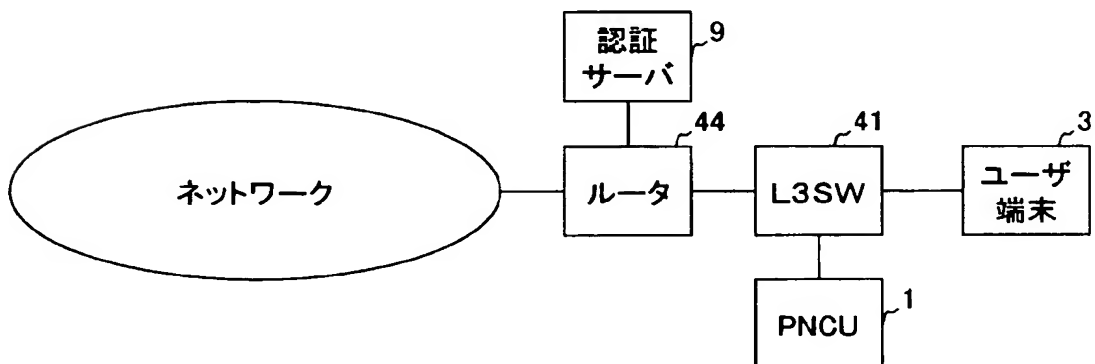
(A) IPv6におけるアクセス自動割当時のアクセス制御



(B) 本発明の実施の形態による解決方法1



(C) 本発明の実施の形態による解決方法2



【図 27】

(A) アドレスリスト

エントリ1	サービスタイプ: IPv6
エントリ2	
⋮	

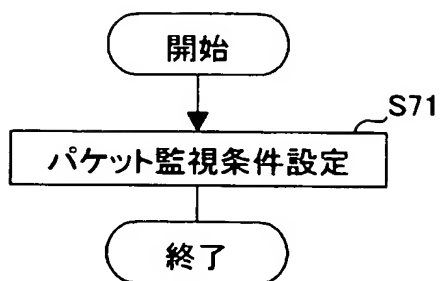
(B) サービス管理テーブル

IPv6 →	処理決定テーブルへの ポインタ1	イベント	処理実体へのポインタ
	処理決定テーブルへの ポインタ2	初期設定	IPv6_INIT
	⋮	アドレス払い出し	IPv6_SET
	⋮	アドレス解放	IPv6_REL
	⋮	タイムアウト	IPv6_REL

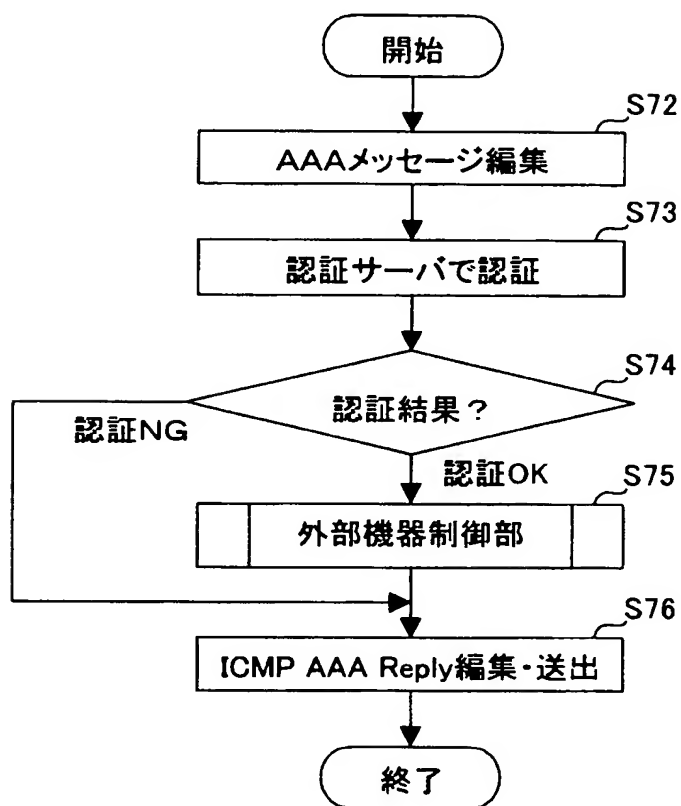
(C) アクセスリスト

IPアドレス	設定情報	状態	外部機器アドレス	タイマ
2000:10::250:56ff:fe15:100	...	規制無し	2000:10::250:56ff:fe15:10	8H
2000:10::250:56ff:fe15:101	...	規制有り	2000:10::250:56ff:fe15:10	...
⋮	⋮	⋮	⋮	⋮

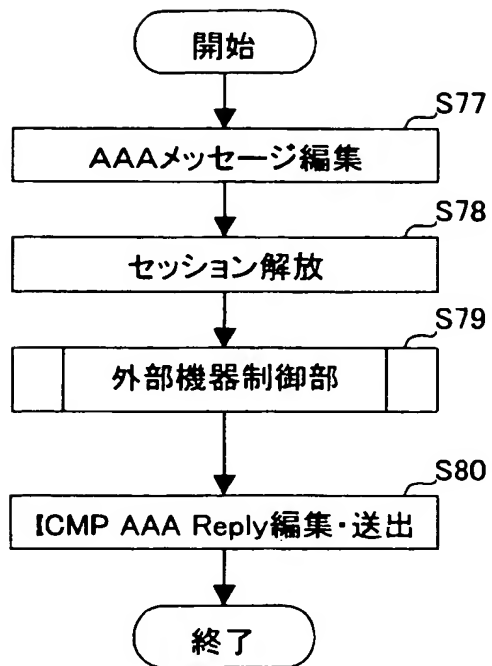
【図 28】



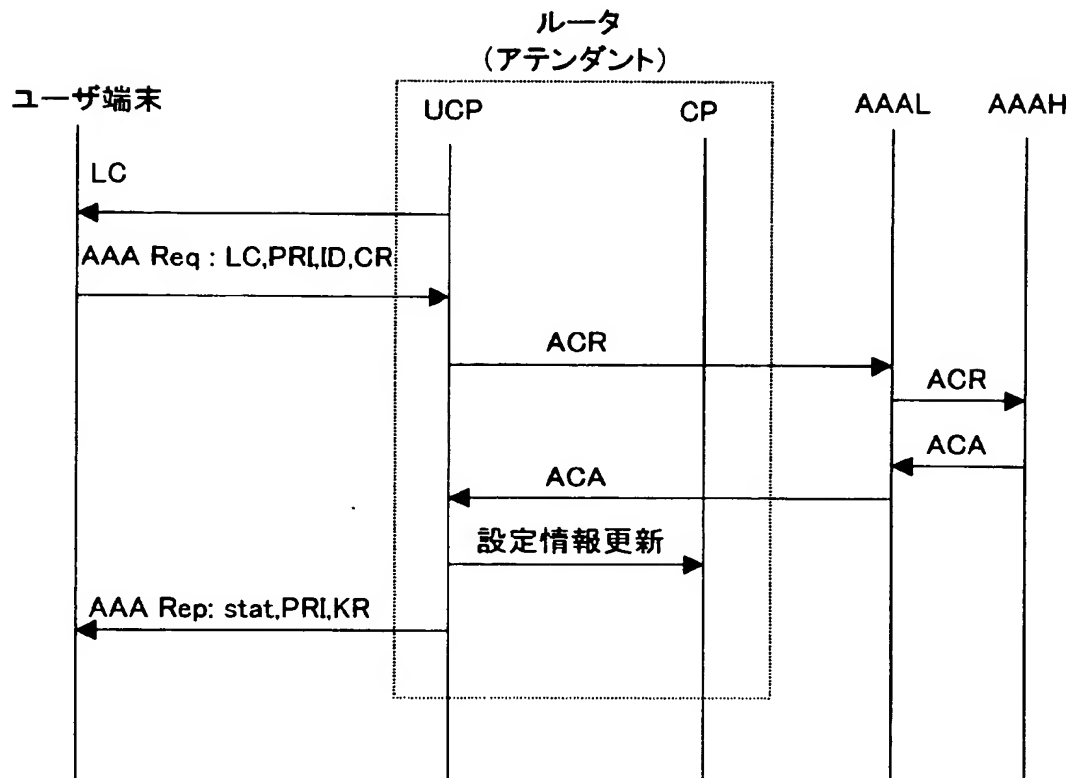
【図 29】



【図 30】



【図 3 1】



LC = ローカル AAA チャレンジ

RPI = ホストと AAAH 間で用いられる再送保護指標

CR = AAA 証明書

ID = クライアント識別子

KR = 鍵応答

UCP = 非制御部分

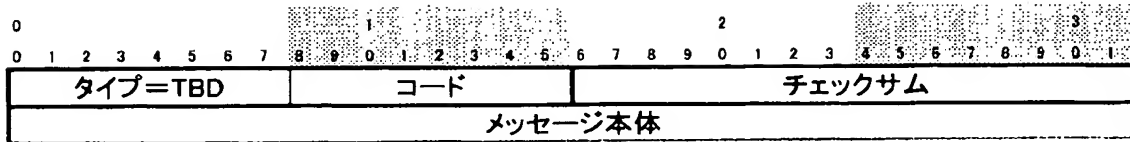
CP = 制御部分

ACR = AAA クライアント要求 (AAA プロトコル使用)

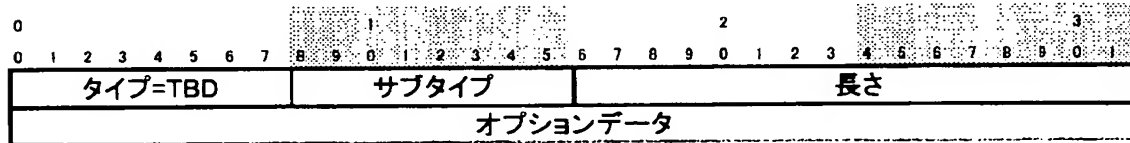
ACA = AAA クライアント応答 (AAA プロトコル応答)

【図 3 2】

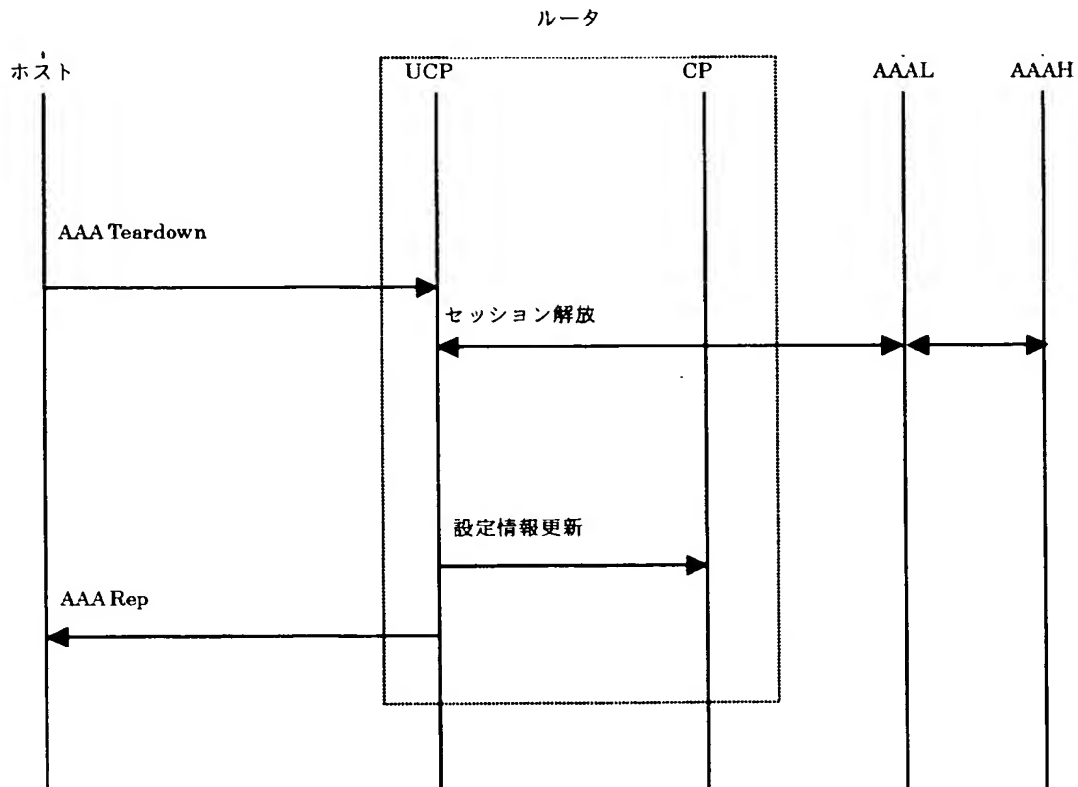
(1) ICMP AAAメッセージ



(2) AAAプロトコルオプション



【図 3 3】



【書類名】 要約書

【要約】

【課題】 ネットワークの既存の装置やネットワークの構成に変更を加えることなく、ネットワークの機能を補完または拡張する。

【解決手段】 ユーザ端末 3 と、ユーザ端末 3 に所定のサービスを提供するサービスサーバ 2 との間で通信されるパケットを監視できる位置に、代理ネットワーク制御装置（PNCU）1 が配置される。PNCU 1 は、ユーザ端末 3 とサービスサーバ 2 との間で通信されるパケットを監視し、該パケットに基づいて、ネットワーク機器 4 1 ～ 4 n の少なくとも 1 つを制御することにより、サービスサーバ 2 の機能を補完または拡張する機能を実行する。たとえば、サービスサーバ 2 が DHCP サーバである場合には、PNCU 1 は、DHCP サーバからユーザ端末 3 に発行された IP アドレスを送信元アドレスとして有するパケットのみが転送されるようにネットワーク機器を制御する。

【選択図】 図 1

特願 2 0 0 2 - 3 4 6 9 4 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

神奈川県川崎市中原区上小田中 1 0 1 5 番地

氏 名

富士通株式会社

2. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社